BGA

BI080135/BI160135

8/16-port IP KVM Switch for PS/2

User Manual

Ver. 1.00

TABLE OF CONTENTS

1. The Quick Installation Guide 4
2. Introduction 7
2.1 When the server is up and running 7
2.2 When the sever is dead 7
2.3 Features 8
2.4 Package contents 9
2.5 Technical specifications 10
2.6 System requirement 11
2.7 Cable diagrams 11
2.8 Product Details 12
3. Hardware installation 13
3.1 Operation Overview 13
3.2 Connecting BI080135/BI160135 to the host system 13
4. Configuration 16
4.1 Initial Configuration 16
4.1.1 Initial configuration via DHCP server 16
4.1.2 Initial configuration via serial console 18
4.1.3 Keyboard, Mouse and Video configuration 18
5. Usage 22
5.1 Prerequisites 22
5.2 Using PS/2 KVM over IP switch as a KVM switch 23
5.2.1 On Screen Display Operation 24
5.2.2 Set PC Port Password 26
5.2.3 Hot Plug 30
5.3 Login into the BI080135/BI160135 and logout 31
5.3.1 Login into the BI080135/BI160135 31
5.3.2 Logout from the BI080135/BI160135 33
5.4 The Remote Console 33
5.5 Main Window 34
5.5.1 Remote Console Control Bar 34
5.5.2 Remote Console Status Lines 43
6. Menu Options 44
6.1 Remote Control 44
6.1.1 KVM Console 44
6.1.2 Telnet Console 45
6.2 Virtual Media 46
6.2.1 Floppy Disk 46
6.2.2 CD ROM 49
6.2.3 Drive redirection 52
6.2.4 Options 58
6.3 User Management 61
6.3.1 Change Password 61

6.3.2 Users And Groups 62
6.4 KVM Settings 64
6.4.1 Users Console 64
6.4.2 Keyboard/Mouse 67
6.4.3 Video 69
6.5 Device Settings **70**
6.5.1 Network 70
6.5.2 Dynamic DNS 72
6.5.3 Security 74
6.5.4 Certificate 77
6.5.5 Serial Port 80
6.5.6 Date And Time 82
6.5.7 Event Log 83
6.6 Maintenance 85
6.6.1 Device Information 85
6.6.2 Event Log 86
6.6.3 Update Firmware 87
6.6.4 Unit Reset 88
7. Troubleshooting 89
8. Certificates 91
FCC 91
CE 91
A. Pin Assignments 92
B. Video Modes 94

1. The Quick Installation Guide Installation

BI080135/BI160135 8-port/16-port PS/2 IP-KVM switch redirects local keyboard, mouse and video data to a remote administration console. All data is transmitted via IP. Besides, BI080135/BI160135 is a KVM switch, which can also be used with a local console. Connecting BI080135/BI160135 to the host system

In order to connect the BI080135/BI160135 perform the following steps:

1. Connect the power supply to BI080135/BI160135.
2. Connect the monitor to the BI080135/BI160135.
3. Connect the keyboard to the BI080135/BI160135.
4. Connect the mouse to the BI080135/BI160135.
5. Plug the HDDB15 pin connector of a 3-in-one cable into any label computer port on the rear of BI080135/BI160135 unit. Then connect the HDDB-15 pin male type for PC video, the purple Mini Din 6 pin female type for keyboard and the green Mini Din 6 pin female type for mouse. To plug these three connectors into the respective ports of computer.
6. Repeat item 5 procedure to all of PC ports of BI080135/BI160135.
7. Connect Ethernet and/or modem, depending how you want to access BI080135/BI160135.

Video modes

BI080135/BI160135 recognizes a limited number of common video modes. When running X-Window on the host system, please don't use any custom mode lines with special video modes. If done so, BI080135/BI160135 may not be able to detect these. You are on the safe side with all standard VESA video modes. Please refer to Appendix C for a list of all known modes.

Initial IP configuration

Initially the BI080135/BI160135 network interface is configured with the parameters shown in Table1.1.

Parameter	Value
IP auto configuration	Fix IP Address
IP-Address	192.168.0.70
Net-mask	255.255.255.0
Default-Gateway	none
IP access control	disabled

Table 1.1: Initial configuration

If this initial configuration doesn't meet your local requirements, you need to do the initial IP configuration. Use one of the following ways:

1. Connect the enclosed NULL modem cable to the serial interface on the rear side. The serial interface needs to be adjusted with the parameters shown in Table 1.2:

Parameter	Value
Bits/second	115200
Data bits	8
Parity	No
Stop bits	1
Flow Control	None

Table 1.2: Serial parameters

Use a terminal software (e.g. hyper term or minicom) to connect to BI080135/BI160135. Reset BI080135/BI160135 and immediately press <ESC>. You will see some device information and a '=>' prompt. Enter the command 'config' and press <Enter>. After waiting a few moments you may configure IP auto configuration, IP address, net mask and default gateway. Pressing <Enter> without entering values does not change settings. The gateway value must be set to 0.0.0.0 (for no gateway) or any other value. You will be asked if the values are correct and get a chance to correct them. After confirming, BI080135/BI160135 performs a reset.

2. Use a crossover Ethernet cable to connect BI080135/BI160135 to a subnet where a DHCP server is available. After the DHCP server has assigned an IP address to BI080135/BI160135 you can use the web interface to configure the device.

Web interface

IP-KVM switch may be accessed using a standard JAVA enabled web browser. You may use the HTTP protocol or a secure encrypted connection via HTTPS. Just enter the configured IP address of IP-KVM switch into your web browser.

Login name	super (factory default)
Password	pass (factory default)

Changing these settings to user specific values is strongly recommended and can be done on the User Management page (see the Section called Users and Groups in Chapter 6).

The Remote Console

The Remote Console is the redirected screen, keyboard and mouse of the remote host system to which BI080135/BI160135 is attached. The web browser who is used for accessing BI080135/BI160135 has to supply a Java Runtime Environment version 1.1 or higher. The Remote Console will behave exactly the same way as if you were sitting directly in front of the screen of your remote system. That means keyboard and mouse can be used in the usual way. Open the console by choosing the appropriate link in the navigation frame of the HTML fronted. Figure 1.3 shows the top of the Remote Console.

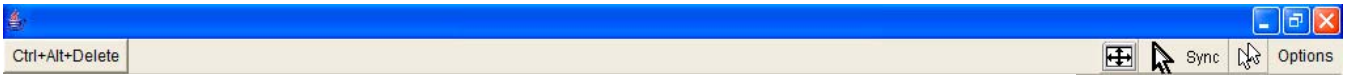


Figure 1.3: Top part of the Remote Console

There are some options to choose from and the important ones are the

following:

Auto Adjust button

If the video displayed is of bad quality or distorted in some way, press this button and wait a few seconds while BI080135/BI160135 tries to adjust itself for the best possible video quality.

Sync Mouse

Choose this option in order to synchronize the local with the remote mouse cursor. This is especially necessary when using accelerated mouse settings on the host system. In general there is no need to change mouse settings on the host.

Video Settings in Options Menu This opens a new window with elements to control the BI080135/BI160135 Video Settings. You can change some values, for instance the brightness and contrast of the picture displayed, which may improve the video quality. It is also possible to revert to the default settings for all video modes or only the current one.

2. Introduction

Thank you for purchasing BI080135/BI160135, PS/2 IP-KVM switch, which can save your MONEY, TIME, SPACE, EQUIPMENT and POWER. BI080135/BI160135 defines a new class of remote KVM access devices. BI080135/BI160135 combines an 8/16-port KVM switch with digital remote KVM access via IP networks and comprehensive system management.

BI080135/BI160135 provides convenient; remote KVM access and control via LAN or Internet. It captures, digitizes, and compresses video signal and transmits with keyboard and mouse signals to and from a remote computer. BI080135/BI160135 provides a non-intrusive solution for remote access and control. Remote access and control software runs on its embedded processors only but not on mission-critical servers, so that there is no interference with server operation or impact on network performance.

BI080135/BI160135 supports consoles consisting of PS/2 style keyboards and mouse, and HD 15 video output. BI080135/BI160135 will automatically detect the current video mode of the console, however manual fine-tuning is recommended to receive the best video quality. BI080135/BI160135 will accept video streams up to 110 MHz dot clock. This results in a screen resolution of 1280x1024 pixels with a frame rate of 60 Hz.

2.1 When the server is up and running

BI080135/BI160135 gives you a full control over the remote server. The Management Console allows you to access the remote server's graphics, keyboard and mouse and to send special commands to the server. You can also perform periodic maintenance of the server. Using the Console Redirection Service, you are able to do the following:

I. Reboot the system.
II. Watch the boot process.
III. Boot the system from a separate partition to load the diagnostic environment.
IV. Run special diagnostic programs.

2.2 When the sever is dead

Obviously, fixing hardware defects is not possible through using a remote management device. Nevertheless BI080135/BI160135 gives the administrator valuable information about the type of a hardware failure. Serious hardware failures can be categorized into five different categories with different chances to happen:

I. Hard disk failure 50%
II. Power cable detached, power supply failure 28%
III. CPU, Controller, main board failure 10%
IV. CPU fan failure 8%
V. RAM failure 4%

Using BI080135/BI160135, administrators can determine which kind of serious hardware failure has occurred (See table 2.1).

Type of failure	Detected by
Hard disk failure	Console screen, CMOS set-up information
Power cable detached, power supply failure	Server remains in power on state after power on command has been given.
CPU Controller, main board failure.	Power supply is on, but there is no video output.
CPU fan failure	By server specific management software
RAM failure	Boot-Sequence on boot console

Table 2.1:Host system failures and how they are detected.

2.3 Features

- 8/16 port KVM switch is 19" rack mount size design.
- Support Microsoft Intellimouse, Microsoft Intellimouse Explorer without user defined key, Logitech Net Mouse or the other fully compatible MS mouse.
- Support Win98SE/2000/ME/XP/Vista, WinNT, Netware, Unix, Linux
- Support iMAC, Power MAC and Sun Microsystems with USB port (Need work with USB-PS/2 adapter)
- Hot Plug - Add PCs or Remove Connected PCs for Maintenance without Powering Down the KVM switch or PCs.
- High Video Quality - Resolution Up To 1920X1440
- No Software Required - easy PC selection via On Screen Display Menu (OSD), Push Buttons, Hot Keys
- At local console side - Support eight characters password protection and search PC server name
- At Remove console side - Use SSL protocol for any encrypted network traffic between itself and a connected client.
- Auto Scan Mode for monitoring PCs and flexible Scan time from 5~255 seconds
- Keyboard status restored when switching PCs
- LED Display for easy status monitoring
- Buzzer sound for switching port confirmation.
- Built-in one extra daisy chain port and no waste any PC port
- Manage serves around the world
- KVM (keyboard, video, mouse) access over IP and analogous telephone line.
- BIOS level access
- No impact on server or network performance
- Automatically senses video resolution for best possible screen capture
- High-performance mouse tracking and synchronization

2.4 Package contents

Model No.: 8 port IP KVM Switch- BI080135

Base unit- 8 port KVM- **BI080135**		1 PC
User's manual		1 PC
AC to DC Power Adapter		1 PC
Rack Mount Kit		1 SET
Daisy Chain Cable		1 PC
3-in-one cables (One HDDB 15-pin male to one 15-pin and two Mini Din 6-pin PS/2 cables)	HDDB	2 PCS
Null modem cable		1 PC
USB A to mini-B Type Cable		1 PC
CD-ROM with supporting programs		1 PC

Model No.: 16 port IP KVM Switch- BI160135

Base unit- 16 port KVM- **BI160135**		1 PC
User's manual		1 PC
AC to DC Power Adapter		1 PC
Rack Mount Kit		1 SET
Daisy Chain Cable		1 PC
3-in-one cables (One HDDB 15-pin male to one 15-pin and two Mini Din 6-pin PS/2 cables)	HDDB	2 PCS
Null modem cable		1 PC
USB A to mini-B Type Cable		1 PC
CD-ROM with supporting programs		1 PC

2.5 Technical specifications

Model No.	8 port KVM- BI080135	16 port KVM- BI160135
PC Port	8	16
Console Port	1	
PC Port Connector (All Female Types)	VGA HDDB 15-pin(shared with PS/2 keyboard and Mouse) USB Type B receptacle	
Console Port Connector (All Female Types)	Local Console: PS/2 Keyboard Mini Din 6 pin PS/2 Mouse Mini Din 6 pin VGA HDDB 15pin Remote Console: RJ-45 8P8C	
Daisy Chain Port Connector (All Female Types)	PS/2 Keyboard mini Din 6 pin PS/2 Mouse Mini Din 6 pin VGA HDDB 15pin	
Serial Port (DB9 pin Male)	1	
LAN port (RJ-45 8P8C)	1 10BASE-T Ethernet uses Category 3/4/5/5E/6 UTP 100BASE-T Ethernet uses Category 5/5E/6 UTP	
Reset port	1	
PC selection	On Screen Display Menu, Hot Key, Push Button	
Bank 7 segment LED	1	
PC Port LED	8	16
On Screen Display Control	Yes	
Scan Intervals	5~255 Sec.	
Keyboard Emulation	PS/2	
Mouse Emulation	PS/2	
VGA Resolution	Local Console: 1920X1440 Remote Console: 1280	
Daisy Chain MAX Level	8 levels	
MAX PC Connection	64	128
Housing	Metal	
Power Adapter	DC 5V, 2.6A	
Operation Temperature	0~50°C	
Storage Temperature	-20 ~ 60°C	
Humidity	0~80%, Non-Condensing	
Size	19" Rack Mount / 1RU	
Weight (kg)	2.0kg	2.2kg
Dimension (cm)	41(L) X 16.4(W) X 4.6(H)	

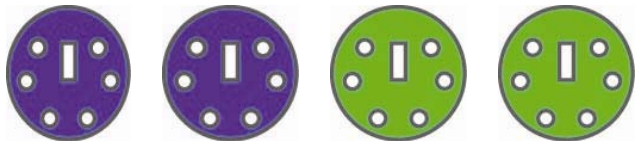
2.6 System requirement

Model No.	**8 ports KVM- BI080135**
Local console side	One VGA Monitor One Keyboard One Mouse
Network Side	10/100Mbps Ethernet or Modem
Remote Console side	One computer
Computer side	8 PCs with 8 3-in-one cables (One HDDB 15-pin male to one HDDB 15-pin and two Mini Din 6-pin PS/2

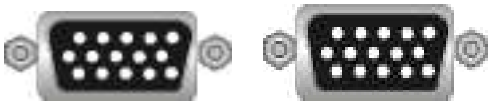
Model No.	**16 ports KVM- BI160135**
Console side	One VGA Monitor One Keyboard One Mouse
Network Side	10/100Mbps Ethernet or Modem
Remote Console side	One computer
Computer side	16 PCs with 16 3-in-one cables (One HDDB 15-pin male to one HDDB 15-pin and two Mini Din 6-pin PS/2 cables)

2.7 Cable diagrams

PS/2 Cable:
Mini Din 6 pin Male to Male

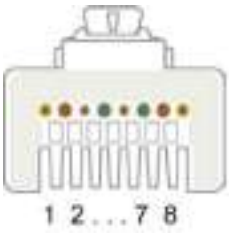


VGA Cable:
HDB15 pin Male to Male



USB 2.0 Cable:
USBA-mini-B

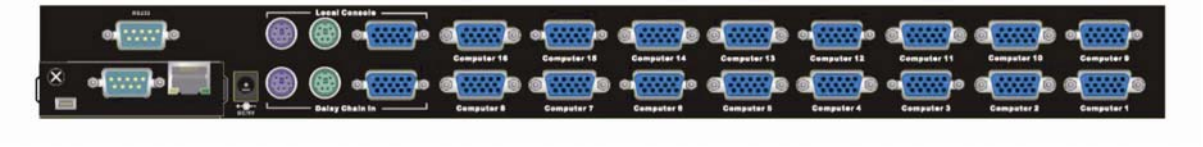
CAT5/5E/6 Straight Through UTP/STP Cable:
8P8C



2.8 Product Details

8 port Rack Mount KVM-BI080135:

16 port Rack Mount KVM-BI160135:



3. Hardware installation

3.1 Operation Overview

Figure 3.1 shows the connections of BI080135/BI160135 to its host, to peripheral devices, to the power source and to the local area network.

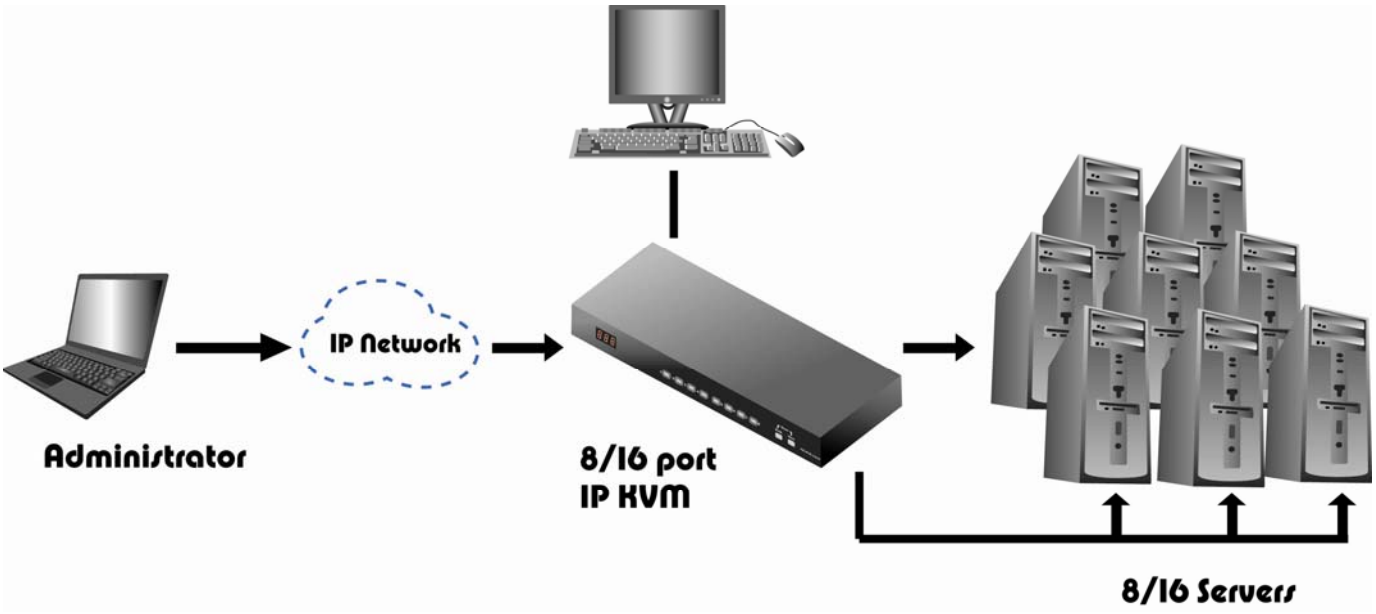


Figure 3.1: BI080135/BI160135 usage scenario

BI080135/BI160135 redirects local keyboard, mouse, and video data to a remote administration console. All data is transmitted via IP.

Attaching one BI080135/BI160135 to a KVM switch or several BI080135/BI160135 to a matrix KVM switch allows accessing multiple servers on a single remote console.

3.2 Connecting BI080135/BI160135 to the host system

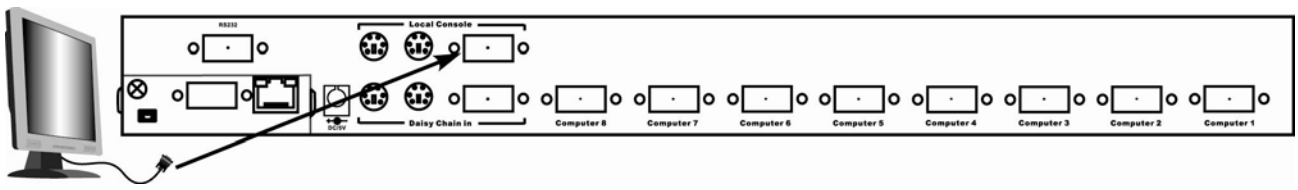
Before installation, please make sure all of peripherals and computers have been turned off. This example of installation is based on Rack Mount BI080135/BI160135. In order to connect the BI080135/BI160135 to the host system, please perform the following steps:

Step 1

Find a convenient place to put your BI080135/BI160135. Its 19" rack mount form factor makes it ideal mountable on 19" rack. When mounting to a rack, attach the included brackets to the sides of the BI080135/BI160135. Take note of the length of your cables so that your computers, KVM Switch, keyboard, mouse and monitor are distanced properly.

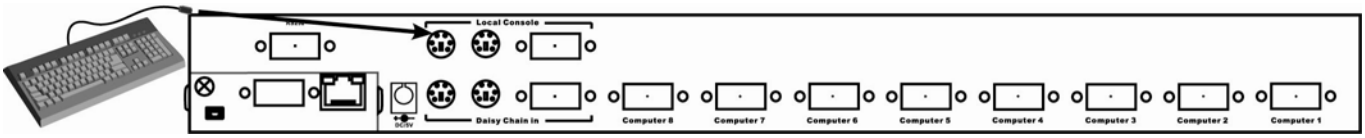
Step 2 (Local console)

Connect the monitor to the KVM Switch. Using the attached cable, or the one included with your monitor, connect it to the HDDB15-pin female port on the back of the KVM unit labeled with the monitor symbol at the CONSOLE connector



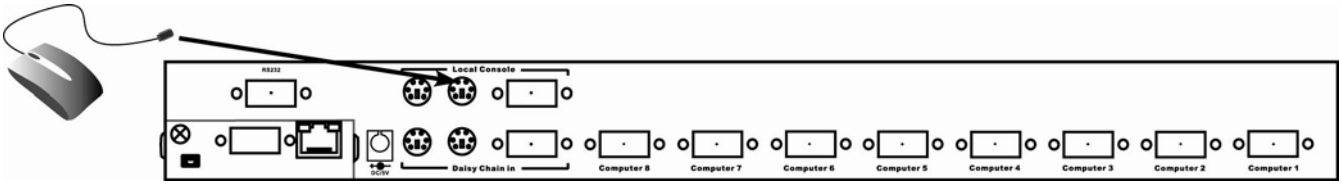
Step 3

Connect the keyboard to the KVM Switch. If you have an AT type keyboard, you will need an AT to PS/2 adapter.



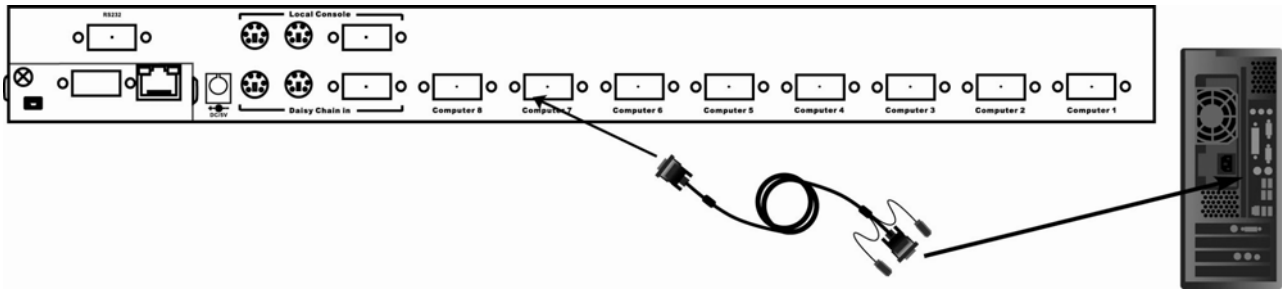
Step 4

Connect the mouse to the KVM Switch.



Step 5

Each PC port connector is HDDB15-pin type. Locate your input cable. It will have an HDDB15-pin male connector at one end. Plug it into any label computer port on the rear of KVM switch unit. The other end of input cable will have three connectors: a HDDB15-pin male type for PC video, a Mini Din 6 pin female type for keyboard and a Mini Din 6 pin female type for mouse. To plug these three connectors into the respective ports of computer. Repeat the same procedure to all of PCs.



Step 6

Double-check all of the connections. You can check the color of keyboard and mouse connector to make sure the keyboard and mouse cables go to the correct ports.

Step 7

Repeat step 5 to 7 for the remainder of the computers

Step 8

Connect the Ethernet and/or modem, **ISDN,** depending how you want to access BI080135/BI160135.

The rear side of BI080135/BI160135 provides a RJ-45 connector for Ethernet. The connector is used either for a 100 Mbps 100BASE-TX connection or for a 10 Mbps 10BASE-T connection. The adapter can sense the connection speed and will adjust to the appropriate operation mode automatically.

10 Mbps Connection

For 10BASE-T Ethernet networks, the Fast Ethernet adapter uses Category 3, 4, or 5 UTP cable. To establish a 10 Mbps connection, the cable must be connected to a 10BASE-T hub.

> Make sure that the cable is wired appropriately for a standard 10BASE-T adapter.
> Align the RJ-45 plug with the notch on the adapter's connector and insert it into the adapter's connector.

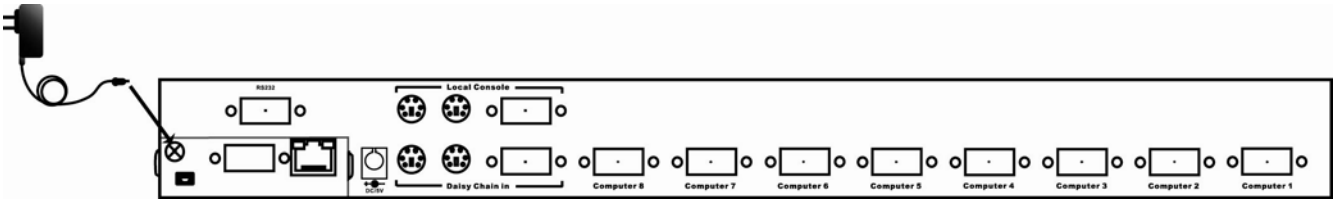
100 Mbps Connection

For 100BASE-TX Fast Ethernet networks, BI080135/BI160135 supports Category 5 UTP cabling. To establish a 100 Mbps connection, the cable must be connected to a 100BASE-TX hub.

> Make sure that the cable is wired appropriately for a standard 100BASE-TX adapter.
> Align the RJ-45 plug with the notch on the adapter's connector and insert it into the adapter's connector.

Step 9

Attach the power supply to the KVM unit and plug the other end into an electrical receptacle.



4. Configuration

4.1 Initial Configuration

The BI080135/BI160135 communication interfaces are all based on TCP/IP. It comes pre-configured with the IP configuration listed in Table 4-1.

Parameter	Value
IP auto configuration	Fix IP Address
IP-Address	192.168.0.70
Net-mask	255.255.255.0
Default-Gateway	None

Table 4-1. Initial network configuration

Warning

If you select DHCP mode, and the DHCP connection fails on boot up, there will be no IP address assigned for BI080135/BI160135.

If this initial configuration does not meet your requirements, the following describes the initial IP configuration that is necessary to access the BI080135/BI160135 for the first time.

4.1.1 Initial configuration via DHCP server

By default, the BI080135/BI160135 will try to contact a DHCP server in the subnet to which it is physically connected. If a DHCP server is found, it may provide a valid IP address, gateway address and net mask. Before you connect the device to your local subnet, be sure to complete the corresponding configuration of your DHCP server. It is recommended to configure a fixed IP assignment to the MAC address of the BI080135/BI160135. You can find the MAC address labeled on the bottom side.

If this initial configuration does not meet your local requirements, use the setup tool to adjust the values to your needs. The setup tool can be found on the CD ROM delivered with this package. You can follow the procedure described below.

BI080135/BI160135 Setup Tool

MAC Address Detection

Connect the BI080135/BI160135 to your computer via local network. Start the setup tool from the CD ROM on the computer that the BI080135/BI160135 is installed. Depending on the connection (USB or network), the device detection is different. A window opens as seen below:

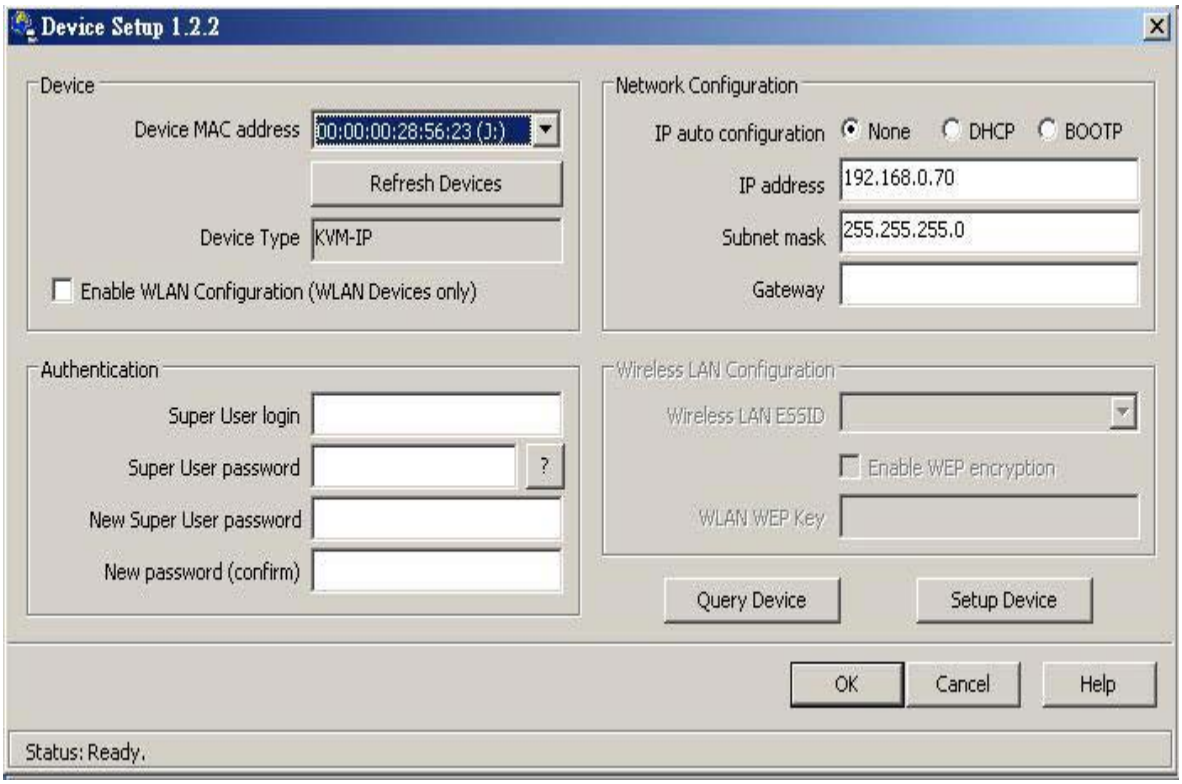


Figure4-1. BI080135/BI160135 switch setup tool

On the upper left corner, the MAC address of the BI080135/BI160135 is displayed. To detect the MAC address, manually, press the button "Refresh Devices". The displayed MAC address is the same MAC address printed on the white sticker placed on the back of the BI080135/BI160135. If the BI080135/BI160135 is connected via USB, it is classified as an USB device and an appropriate drive letter is chosen for this device.

On the lower right corner of the window, there are two buttons: "Query Device" and "Setup Device". Press the "Query Device" button to display the preconfigured values of the network configuration. The values are displayed in the text fields located above. If necessary, adjust the network settings to your needs. To save the changes enter an user name and an according password. Then press the " Setup Device " button.

Authentication

To adjust the authentication settings, enter your login as a super user, and change your password.

Super user login
Enter the login name of the super user. The initial value is " super ". All of characters are lower case.

Super user password
Enter the current password for the super user. This initial value is " pass ". All of characters are lower case.

New super user password Enter the new password for the super user.

New password (confirm) Re-type the new password for the super user.

To close the window and accept the changes, press the " OK " button, otherwise press the " Cancel " button.

4.1.2 Initial configuration via serial console

Using a serial terminal, the BI080135/BI160135 has a serial line interface (rear side). This connector is compliant with the RS 232 serial line standard. The serial line has to be configured with the parameters given in Table 4-2.

When configuring with a serial terminal, reset the BI080135/BI160135 and immediately press the "ESC" key. You will see some device information, and a "=>" prompt. Enter "config", press "Enter" and wait for a few seconds for the configuration questions to appear.

Parameter	Value
Bits/second	115200
Data bits	8
Parity	No
Stop bits	1
Flow Control	None

Table 4-2. Serial line parameters

As you proceed, the following questions will appear on the screen. To accept the default values which are shown in square brackets below, press "Enter".

IP auto configuration (non/dhcp/bootp) [dhcp]:
IP [192.168.0.70]:
Net mask [255.255.255.0]:
Gateway (0.0.0.0 for none) [0.0.0.0]:

IP autoconfiguration

With this option, you can specify whether the BI080135/BI160135 should get its network settings from a DHCP or BOOTP server. For DHCP, enter "DHCP", and for BOOTP enter "bootp". If you do not specify any of these, the IP auto configuration is disabled and subsequently you will be asked for the following network settings.

IP address

The IP address the BI080135/BI160135 uses. This option is only available if IP auto configuration is disabled.

Net mask

The net mask of the connected IP subnet. This option is only available if IP autoconfiguration is disabled.

Gateway address

The IP address of the default router for the connected IP subnet. If you do not have a default router, enter 0.0.0.0. This option is only available if IP autoconfiguration is disabled.

4.1.3 Keyboard, Mouse and Video configuration

Between the BI080135/BI160135 and the host, there are two interfaces available for transmitting keyboard and mouse data: USB and PS/2. The correct operation of the remote mouse depends on several settings, which will be discussed in the following subsections.

Warning

Only the PC with USB connection to BI080135/BI160135 could support both PS/2 and USB. All the other PCs could support PS/2 only.

4.1.3.1 BI080135/BI160135 keyboard settings

The BI080135/BI160135 settings for the host's keyboard type have to be correct in order to make the remote keyboard work properly. Check the settings in the BI080135/BI160135 front-end.

4.1.3.2 Remote Mouse Settings

A common problem with KVM devices is the synchronization between the local and remote mouse cursors. The BI080135/BI160135 addresses this situation with an intelligent synchronization algorithm. There are two mouse modes available on the BI080135/BI160135.

Auto mouse speed

The automatic mouse speed mode tries to detect the speed and acceleration settings of the host system automatically. See the section below for a more detailed explanation.

Fixed mouse speed

This mode just translates the mouse movements from the Remote Console in a way that one pixel move will lead to n pixel moves on the remote system. This parameter n is adjustable with the scaling. It should be noted that this works only when mouse acceleration is turned off on the remote system.

4.1.3.3 Auto mouse speed and mouse synchronization

The automatic mouse speed mode performs the speed detection during mouse synchronization. Whenever the mouse does not move correctly, there are two ways for re-synchronizing local and remote mouse:

Fast Sync

The fast synchronization is used to correct a temporary, but fixed skew. Choose the option using the Remote Console options menu or press the mouse synchronization hotkey sequence in case you defined one.

Intelligent Sync

If the fast sync does not work or the mouse settings have been changed on the host system, use the intelligent resynchronization. This method takes more time than the fast one and can be accessed with the appropriate item in the Remote Console option menu. The intelligent synchronization requires a correctly adjusted picture. Use the auto adjustment function or the manual correction in the Video Settings panel to setup the picture. The Sync mouse button on top of the Remote Console can behave differently, depending on the current state of mouse synchronization. Usually pressing this button leads to a fast sync, except in situations where the KVM port or the video mode changed recently.

Note: At first start, if the local mouse pointer is not synchronized with the remote mouse pointer, press the Auto Adjust Button once.

4.1.3.4 Host system mouse settings

The host's operating system knows various settings from the mouse driver.

Warning

The following limitations are not for the Mouse Type of "MS Windows 2000 and newer".

While the BI080135/BI160135 works with accelerated mice and is able to synchronize the local with the remote mouse pointer, there are the following limitations, which may prevent this synchronization from working properly:

Special Mouse Driver

There are mouse drivers which influence the synchronization process and lead to desynchronized mouse pointers. If this happens, make sure you do not use a special vendor-specific mouse driver on your host system.

Windows XP Mouse Settings

Windows XP knows a setting named "improve mouse acceleration", which has to be deactivated.

Active Desktop

If the Active Desktop feature of Microsoft Windows is enabled do not use a plain background. Instead, use some kind of wallpaper. As an alternative, you could also disable the Active Desktop completely.

Navigate your mouse pointer into the upper left corner of the applet screen and move it slightly forth and back. Thus the mouse will be resynchronized. If re-synchronizing fails, disable the mouse acceleration and repeat the procedure.

4.1.3.5 Single and Double Mouse Mode

The information above applies to the Double Mouse Mode, where remote and local mouse pointers are visible and need to by synchronize. The BI080135/BI160135 also features another mode, the Single Mouse Mode, where only the remote mouse pointer is visible. Activate this mode in the open Remote Console and click into the window area. The local mouse pointer will be hidden and the remote one can be controlled directly. To leave this mode, it is necessary to define a mouse hotkey in the Remote Console Settings Panel. Press this key to free the captured local mouse pointer.

4.1.3.6 Recommended Mouse Settings

For the different operating systems we can give the following advice:

MS Windows 2000/2003 (Professional and Server), XP

In general, we recommend the usage of a mouse via USB. Choose USB without Mouse Sync. For a PS/2 mouse choose Auto Mouse Speed. For XP disable the option enhance pointer precision in the Control Panel.

SUN Solaris

Adjust the mouse settings either via xset m 1 or use the CDE Control Panel to set the mouse to 1:1, no acceleration. As an alternative you may also use the Single Mouse Mode.

MAC OS X

We recommend using the Single Mouse Mode.

4.1.3.7 Video Modes

The BI080135/BI160135 recognizes a limited number of common video modes. When running X11 on the host system, please do not use any custom mode lines with special video modes. If you do, the BI080135/BI160135 may not be able to detect them. We recommend using any of the standard VESA video modes, instead

5. Usage

5.1 Prerequisites

The BI080135/BI160135 features an embedded operating system and applications offering a variety of operating interfaces. This chapter will describe both these interfaces, and the way to use them in a more detailed manner. The interfaces are accessed using the TCP/IP protocol family, thus they can be accessed using the built-in Ethernet adapter.

The following interfaces are supported:

HTTP/HTTPS

You can full access the device via the embedded web server. The BI080135/BI160135 environment can be entirely managed using a standard web browser. You can access the BI080135/BI160135 using the insecure HTTP protocol, or using the encrypted HTTPS protocol. Whenever possible, use HTTPS.

Telnet

A standard Telnet client can be used to access an arbitrary device connected to the BI080135/BI160135 serial port via a terminal mode.

The primary interface of the BI080135/BI160135 is the HTTP interface. This is covered extensively in this chapter. Other interfaces are addressed in subtopics.

In order to use the Remote Console window of your managed host system, the browser has to come with a Java Runtime Environment version 1.1 or higher. If the browser has no Java support (such as on a small handheld device), you are still able to maintain your remote host system using the administration forms displayed by the browser itself.

Important: We recommend installing a Sun JVM 1.4 or higher.

In order to access the remote host system using a securely encrypted connection, you need a browser that supports the HTTPS protocol, such as IE 6.0. Strong security is only assured by using a key length of 128 Bit. Some of the old browsers do not have a strong 128 Bit encryption algorithm.

Using the Internet Explorer, open the menu entry "?" and "Info" to read about the key length that is currently activated. The dialog box contains a link that leads you to information on how to upgrade your browser to a state of the art encryption scheme. Figure 5-1 shows the dialog box presented by the Internet Explorer 6.0.

Figure 5-1. The Internet Explorer displaying the encryption key length

Newer web browsers do support strong encryption on default.

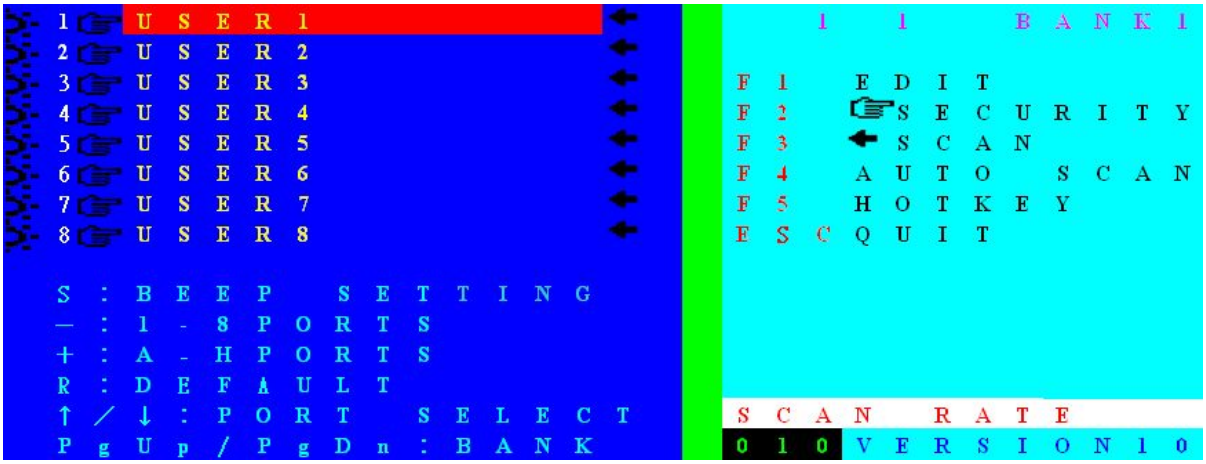
5.2 Using PS/2 KVM over IP switch as a KVM switch

5.2.1 At factory default the PS2 KVM will not ask for password unless it is set by user. You may press "**Scroll Lock**" twice followed by "**F2**" to bring up password setting menu.

★ NOTE : Before you are familiarized with this device, it is strongly recommended to use without password. If password is forgotten, please send PS2 KVM to your distributor for factory reset.

5.2.2 To switch port, you may enter OSD menu to select port, or, use Hot-Key to perform switching. To bring up OSD menu, please press "**Scroll Lock**" twice to activate OSD Main Menu as illustrated below**<fig.5-2>.**

OSD Main Menu



<fig.5-2>

5.2.3 OSD Main Screen Headings

	indicates the computer is powered on at selected port
☞	indicates the computer attached at this port has password protected. All ports at factory default do not have password assigned, therefore no icon present
USER1~8	Port name of corresponding port number. USER 1~8 illustrated as factory default setting.
	indicates the PC port is set for Auto Scn Mode. At factory default all PC port is active for Auto Scan.
S	Every time switching is made PS2 KVM beeps for notification. Please press Scroll Lock twice followed by “S” to turn beeper on or off
–	to select 1~8 computer Ports (1~8 PC Port)
+	to select A~H computer port (9~16 PC Port)
R	to set factory default. (★ NOTE: password will not be erased after this operation)
↑	Select computer at previous port
↓	Select computer at next port
PgUp	Select previous bank
PgDn	Select next bank
1 1	Left hand side ”1” indicates current active port, right hand side “1” indicates current active bank.
F1	Edit computer name
F2	Password setting
F3	Select scan port
F4	Auto scan mode
F5	Hot key setting
ESC	Exit OSD
SCAN RATE	Scan rate
VERSION	Firmware version

5.2.3.1 Use right hand side of OSD commands for adjust settings
Function keys: **F1, F2, F3, F4, F5, ESC and → left arrow key**

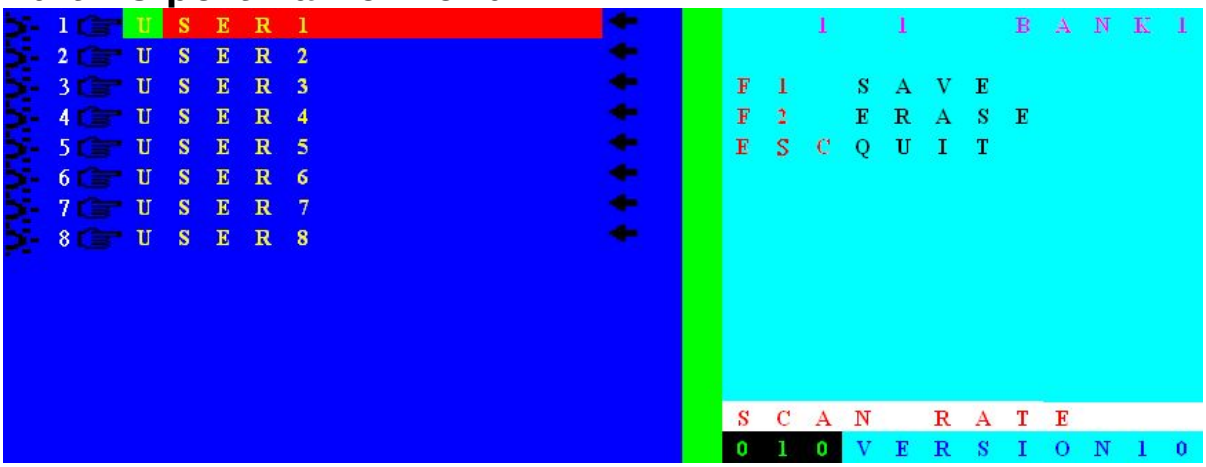
- First row on right hand window – "1 1 Bank1" : indicates currently PS2 KVM active at Bank 1, computer port 1.
- SCAN RATE set at 10 second
- Firmware version now at version 1.0

F1 Edit computer name (EDIT)
On the OSD menu, please press F1 to edit PC port name as illustrated below <fig.5-3>.

Now please use the secondary function key to **F1(SAVE), F2(ERASE), or ESC(QUIT)**

- Edit the desirable name at cursor position, maximum 12 characters.
- F1- Save port name settings and brings back to OSD main menu
- F2- Erase all texts. To erase individual character, please use Backspace (←)
- ESC to exit EDIT menu

Edit PC port name menu

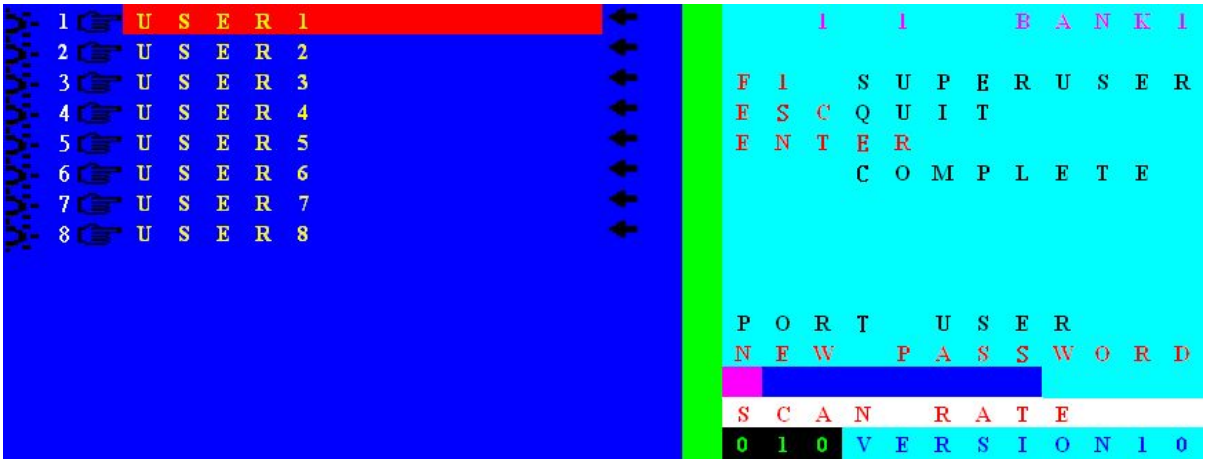


<fig.5-3>

F2- Password setting (SECURITY)
Press F2 at OSD main menu to activate password setting (☞ SECURITY). Password setting menu for "PORT USER" pops up as illustrated below <fig.5-4>. In this screen you may use the secondary OSD function keys: **F1(SUPERUSER), ESC(QUIT), ENTER(Complete)**.

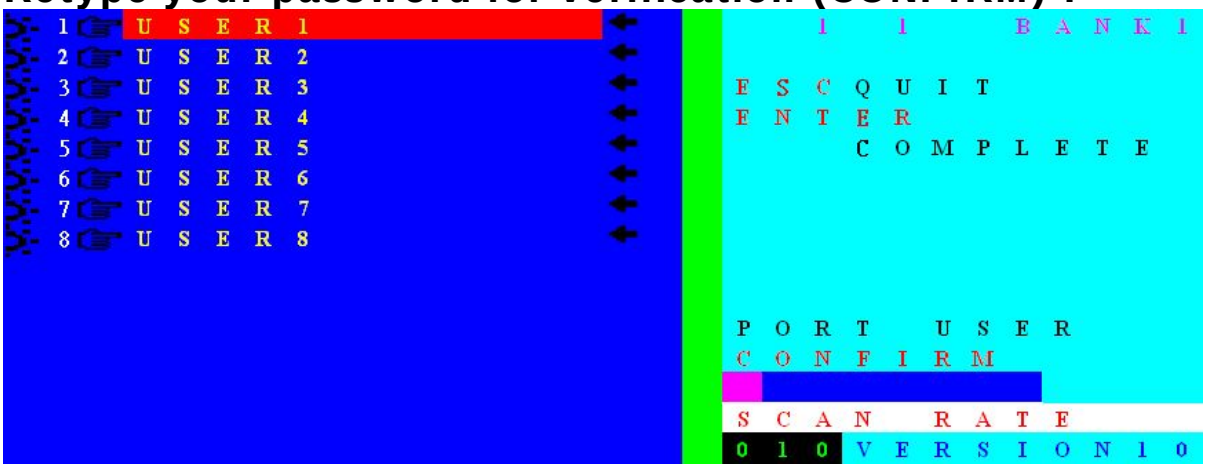
- **F1**- To set password please press F1(SUPERUSER) to set SUPERUSER password <fig.5-6>
  No password for SUPERUSER is set at factory default. Please enter password of maximum 8 characters. To remove SUPERUSER password, press ENTER at "New Password" field.
- **ENTER**- Press ENTER to complete settings
- **ESC**- When setting is finished, press ESC return to OSD main menu.

Set PC Port Password :



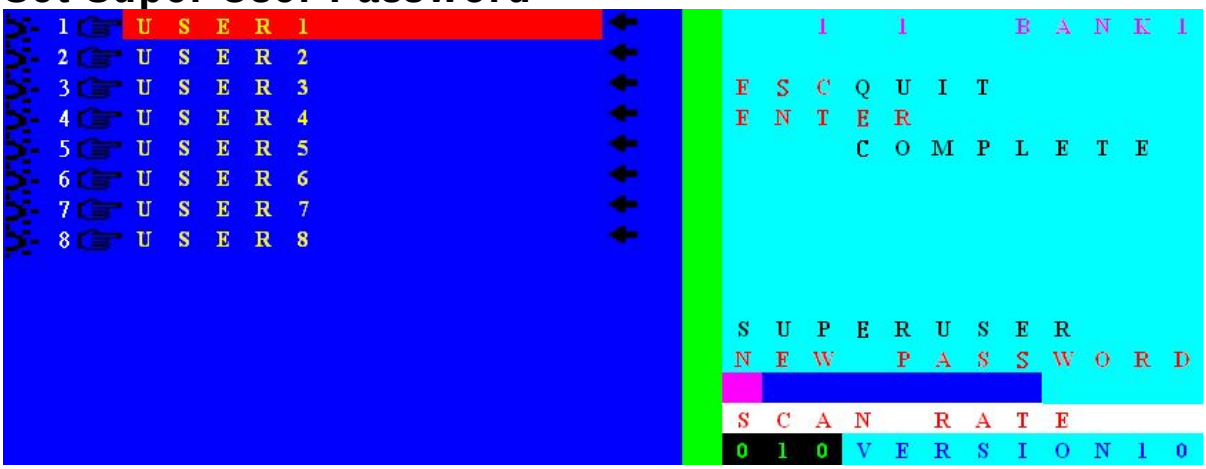
<fig.5-4>

Retype your password for verification (CONFIRM) :



<fig.5-5>

Set Super User Password



<fig.5-6>

PC port without Password illustrated below <fig.5-7>**:**

<fig.5-7>

At factory default, no password is set for PS2 KVM Switch as illustrated above.

Selected PC port is powered on with indication.

To setup password please open OSD, select SECURITY. Please refer to <fig.5-4> and <fig.5-5>

PC port with password illustrated below <fig.5-8>**:**

<fig.5-8>

Password request OSD appears for Port-1 computer with powered on status. Enter password directly. Password allowable length at 1 to 8 characters only (8 characters max). Press ENTER after password input to commence operation for this PC.

SUPERUSER PASSWORD illustrated below <fig.5-9>**:**

<fig.5-9>

If SUPERUSER password is set, PS2 KVM Switch will ask for password when KVM is powered on or at RESET. Please enter password follow by ENTER key to continue operation.

F3- SELECT SCAN PORT

Press F3 at OSD main menu to select Auto Scan active port. If a port is selected for Auto Scan, a icon appears, press F3 again, the icon will disappear.

F4- AUTO SCAN

Press F4 at OSD main menu to enter Auto Scan function menu as illustrated below <fig.5-10>. The secondary function keys are F1, F2 and F3

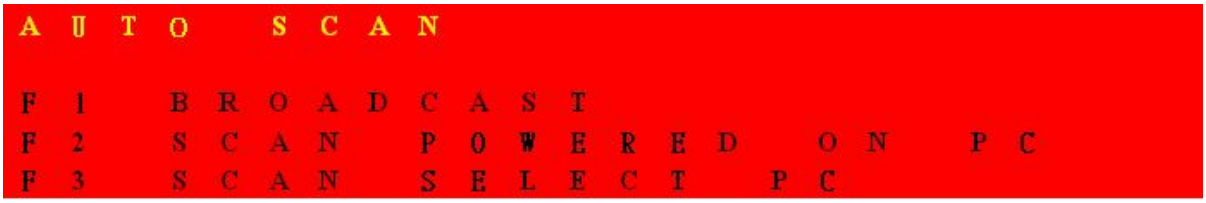
- F1- To start complete scanning, please press F1 (BROADCAST). All ports will be scanned regardless whether the port is connected with active computer. The scanning process will be stopped when ESC is pressed. As scan terminates, KVM switch maintains at last scanned PC port OSD.

- F2- To start scanning powered on PC only, please press F2 (POWERED ON PC). To stop scanning, please press ESC button. As scan terminates, KVM switch maintains at last scanned PC port OSD.

- F3- To scan selected PC, please press F3 (SCAN SELECT PC) to commence scanning. To stop scanning, please press ESC button. As scan terminates, KVM switch maintains at last scanned PC port OSD.

- ESC- Press ESC to Exit the Auto Scan menu.

AUTO SCAN



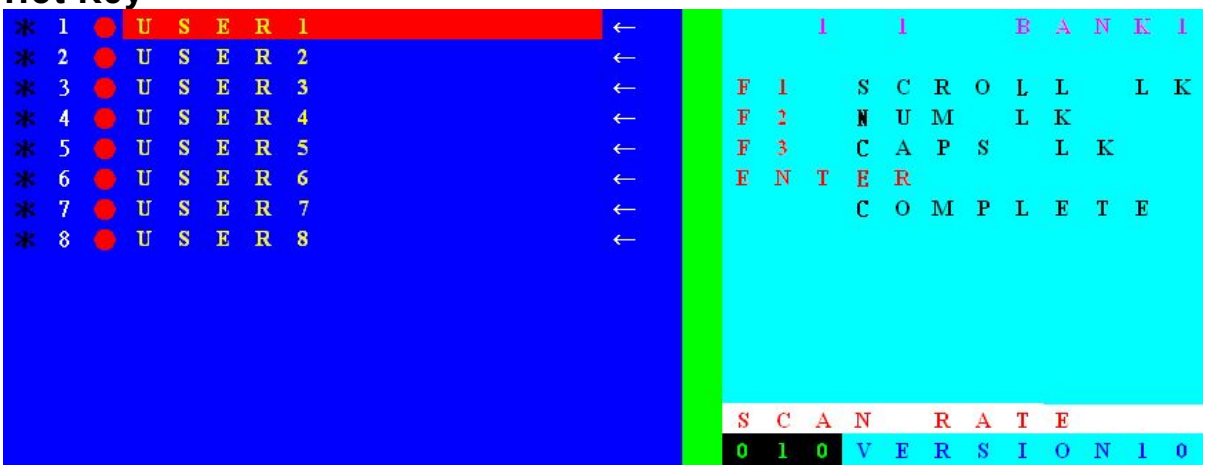
<fig. 5-10>

F5- HOT-KEY

At OSD main menu, please press F5 to enter HOT-KEY setting menu <fig.5-11>. In the HOT KEY setting menu, secondary selection keys are F1, F2, F3, ENTER.

- Press **F1** to select Scroll Lock as Hot-key
- Press **F2** to select Num Lock as Hot-key
- Press **F3** to select Caps Lock as Hot-key
- Press **ENTER** to save setting and exit the Hot-key setting menu

Hot Key



<fig.5-11>

OSD RATE / SCAN RATE SETTING

To set scan rate please press ⟶ button to enter Scan Rate/OSD Rate setting menu as illustrated below <fig.5-12>. The secondary menu functions are F1 and ENTER button

SCAN RATE SETTING

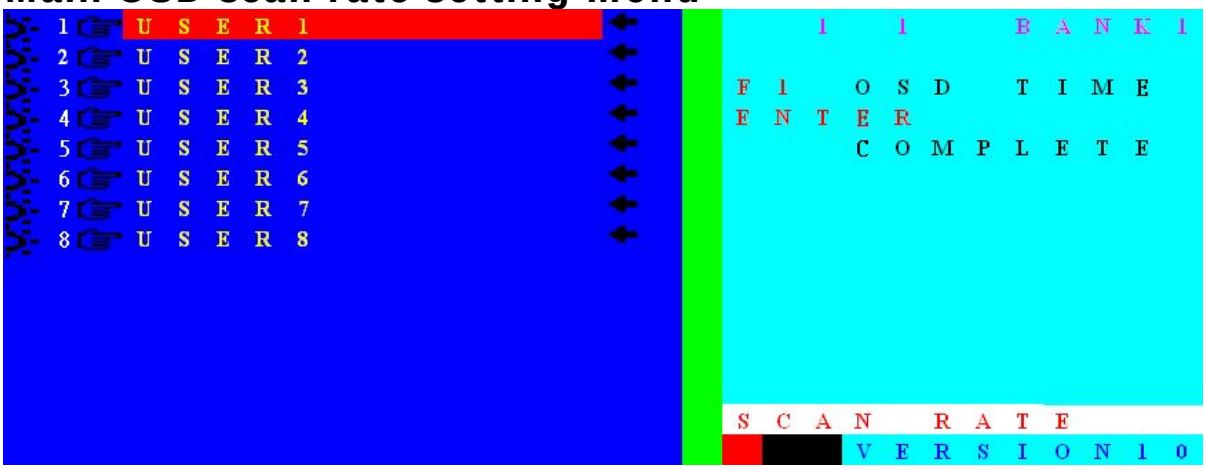
Please note that scan rate is set 10 seconds at factory default. Please enter desirable time interval (005~255 seconds) in the cursor and press ENTER to confirm setting.

OSD RATE SETTING

- Press F1 to enter OSD TIME setting screen <fig.5-13>. Please enter OSD RATE at bottom right corner (005~255 seconds).
- Press ENTER to complete setting (005~255 seconds) and returns to OSD main menu.
- Please press ESC to clear OSD display if OSD Time is not set. When OSD Time is set, please wait until setting time terminates. Note that ESC button OSD cancellation cannot be used when OSD Time is set.

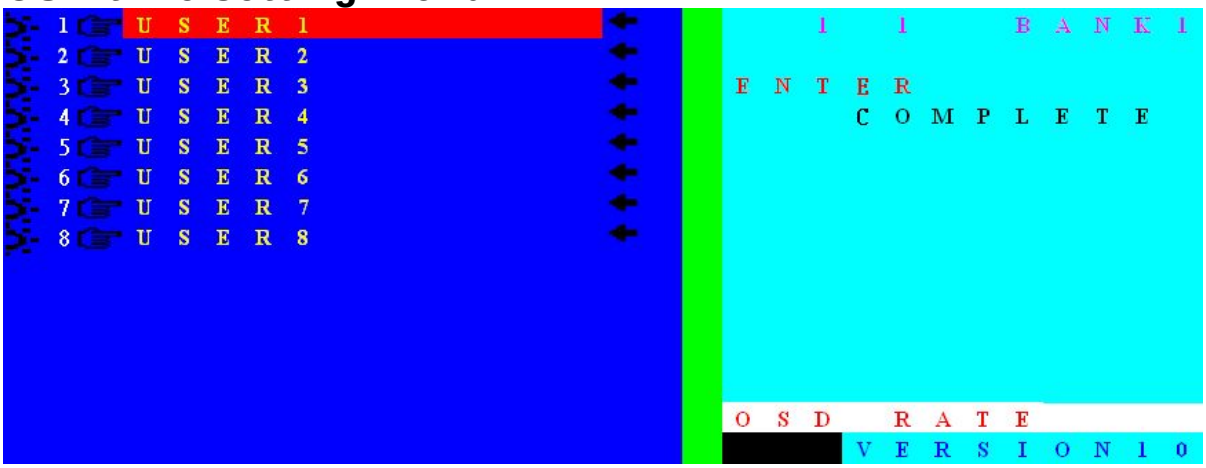
NOTE: When entering OSD RATE and SCAN RATE please enter complete three digits. For example, to enter 5 seconds, please input 005; to enter 10 seconds, please input 010.

Main OSD scan rate setting menu



<fig.5-12>

OSD time setting menu



<fig.5-13>

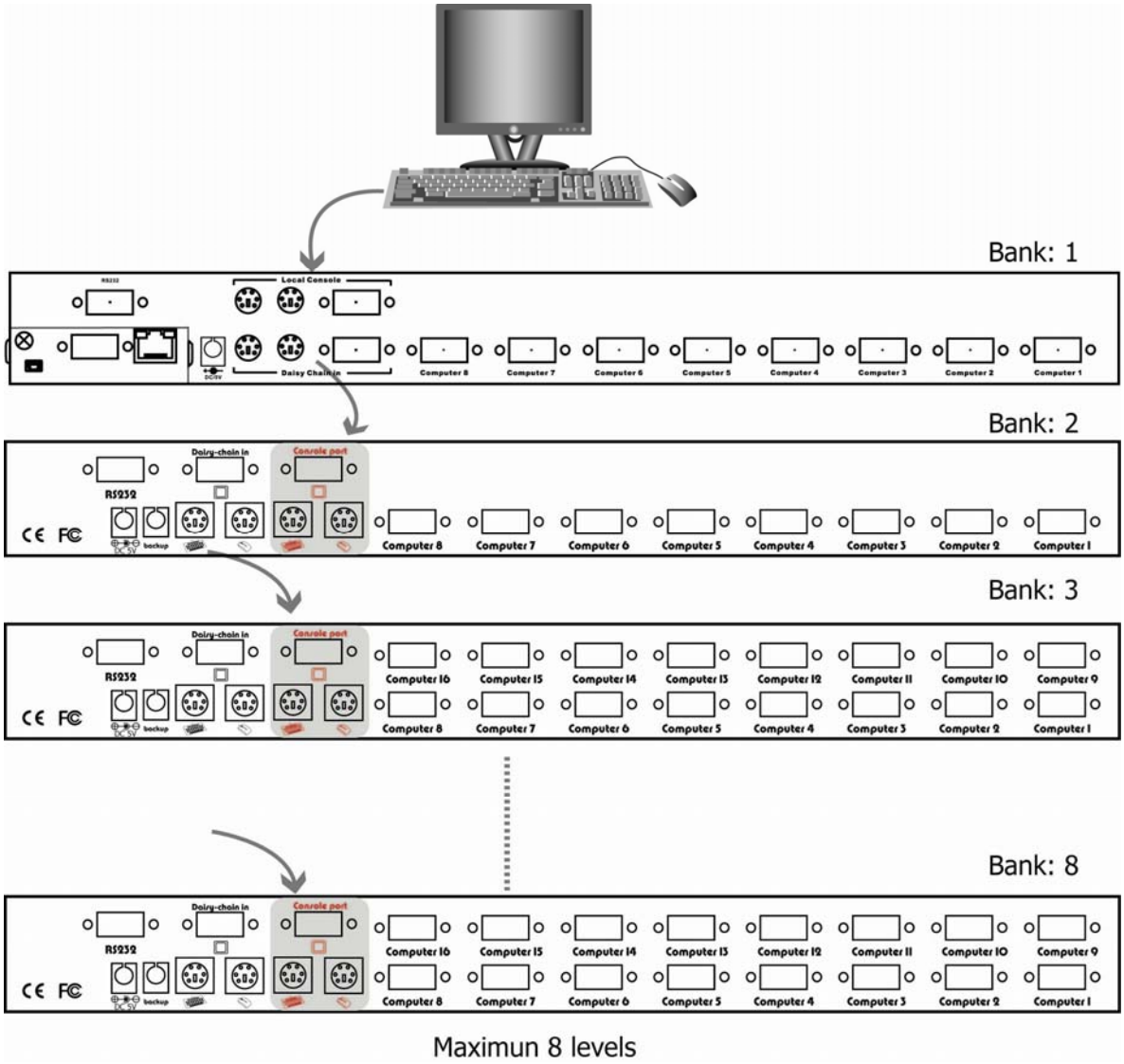


Figure 5-2: Daisy Chain Connection

5.2.3.2 Hot Plug

The KVM Switch supports "Hot Plug" function for easy addition or removal of PCs. The user can arrange or maintain PCs as follows:

a. A PC can be disconnected and reconnected to the same or different port of the KVM unit without having to power it off as long as it is not the Daisy-chain port or pass through port.

b. When the pass through port PC (i.e. The pass through port means the PC port that is connected to console port directly) is powered on, for hot plug function, please switch this pass through port to next port (or say emulation port) and then switch back to the pass through port.

c. You may unplug or plug the mouse or the keyboard from the console port any time.

NOTE:

Some O.S. (Operation Systems) like SCO Unix are unable to support " Hot Plug " function. If you apply "Hot Plug" to this kind of O.S., it will cause unpredictable behavior or shut down the PC. Before attempting to use "Hot Plug", please make sure your O.S. and mouse software driver supports the "Hot Plug" function.

5.3 Login into the BI080135/BI160135 and logout

5.3.1 Login into the BI080135/BI160135

Launch your web browser. Direct it to the address of your BI080135/BI160135, which you configured during the installation process. The address might be a plain IP address or a host/domain name, in case you had given your BI080135/BI160135 a symbolic name in the DNS. For instance, type the following strings in the address line of your browser when establishing an unsecured connection:

http://<IP address of PS/2 IP-KVM>

When using a secure connection, type in:

https://<IP address of PS/2 IP-KVM>

This will lead you to the BI080135/BI160135 login page as shown in Figure 5-3.

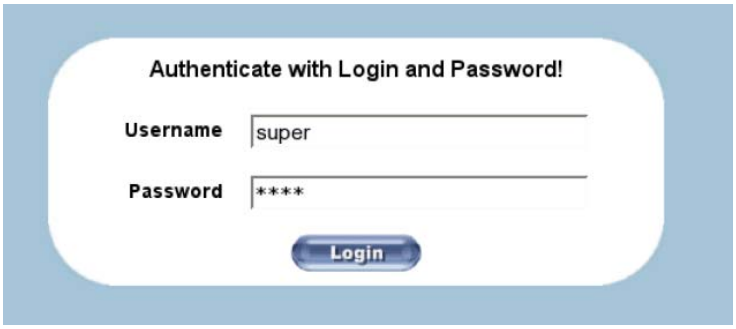


Figure 5-3. Login screen

The BI080135/BI160135 has a built-in super user that has all permissions to administrate your BI080135/BI160135:

Login name	super (factory default)
Password	pass (factory default)

Table 5-1. Standard user settings

Warning

The user “super” is not allowed to login via the serial interface of the IP-KVM.

Warning

Please make sure to change the super user password immediately after you have installed and accessed your IP-KVM for the first time. Unchanging of the password for the super user is a severe security risk and might result in unauthorized access to the IP-KVM and to the host system including all possible consequences!

Warning

Your web browser has to accept cookies, or else login is not possible.

Navigation

After logged in the BI080135/BI160135 successfully, the main page of the BI080135/BI160135 will appear (see Figure 5-4). This page consists of three parts; each of them contains specific information. The buttons on the upper side allow you to navigate within the front end (see Table 5-2 for details). The lower left frame contains a navigation bar and allows you to switch between the different sections of the BI080135/BI160135. Within the right frame, task-specific information is displayed.

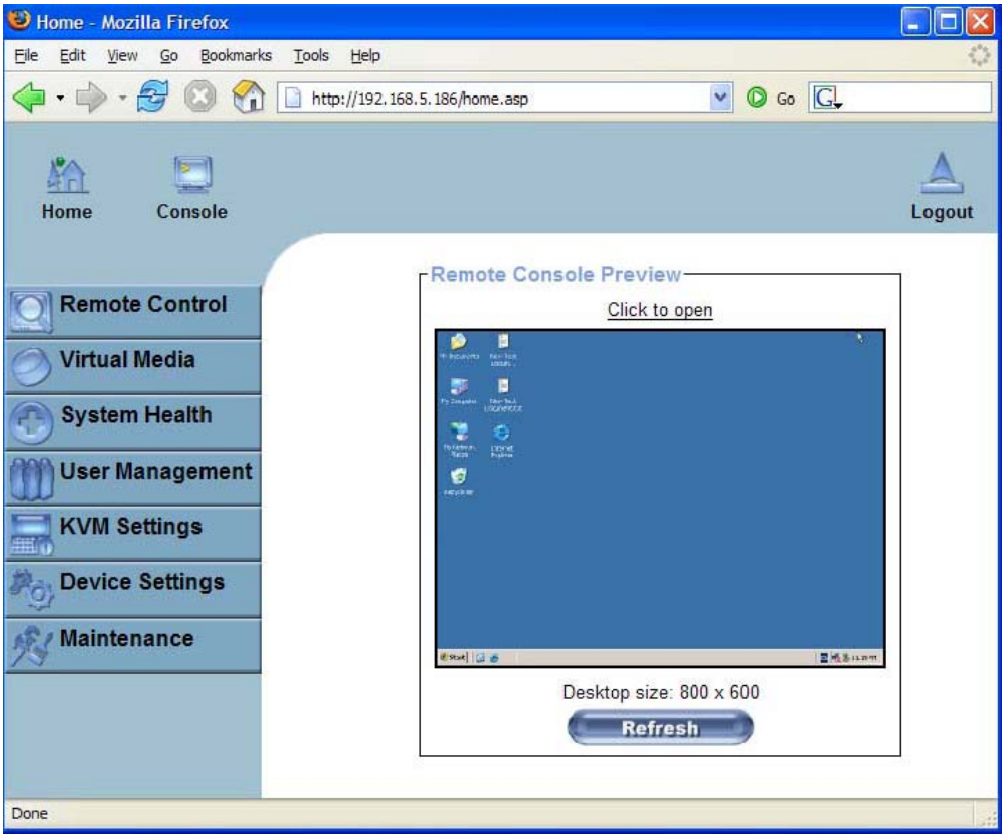


Figure 5-4. Main page

Table 5-2. Buttons from the front end

	Return to the main page of the BI080135/BI160135 .
	Open the BI080135/BI160135 remote console.
	Exit from the BI080135/BI160135 front end.

Warning

If there is no activity for 30 minutes, the IP-KVM will log you out, automatically. A click on one of the links will bring you back to the login screen.

5.3.2 Logout from the BI080135/BI160135

This link logs out the current user and presents a new login screen. Please note that an automatic logout will be performed in case there is no activity for half an hour.

5.4 The Remote Console

General description

The Remote Console is the redirected screen, keyboard and mouse of the remote host system that BI080135/BI160135 controls.

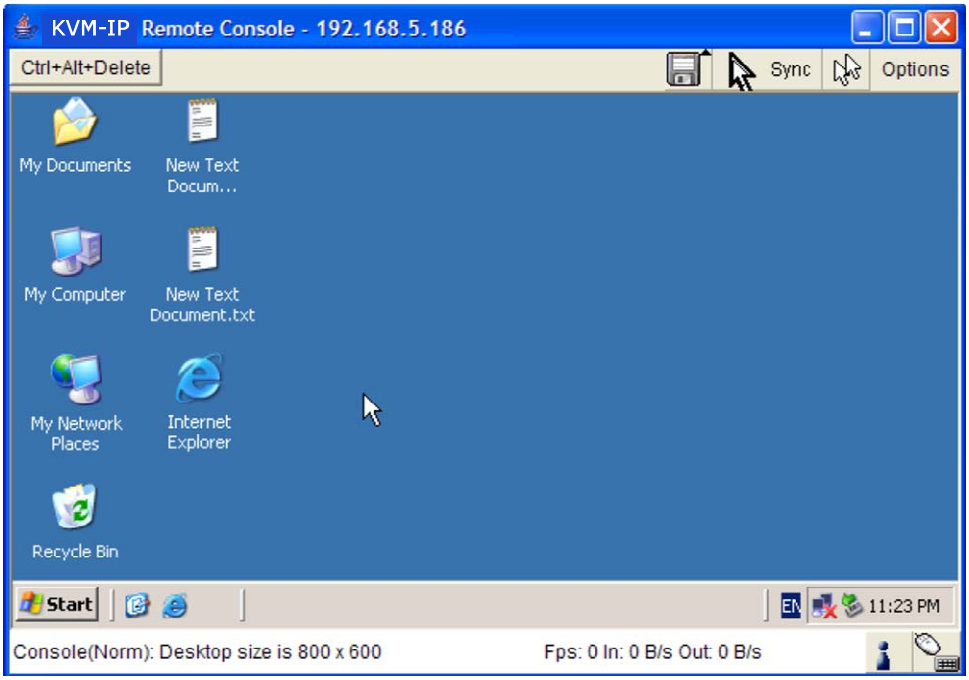


Figure 5-5. Remote Console

The Remote Console window is a Java Applet that tries to establish its own TCP connection to the BI080135/BI160135. The protocol that is run over this connection is neither HTTP or HTTPS, but RFB (Remote Frame Buffer Protocol). Currently, RFB tries to establish a connection to port number 443. Your local network environment has to allow this connection to be made, i.e. your firewall and, in case you have a private internal network, your NAT (Network Address Translation) settings have to be configured accordingly.

If the BI080135/BI160135 is connected to your local network environment and the connection to the Internet is via proxy server without configuring NAT, the Remote Console will not be able to establish the according connection. The reason is that the web proxies are not capable of relaying the RFB protocol.

If the problems above happen, please consult your network administrator in order to provide an appropriate network environment.

5.5 Main Window

Clicking the Remote Console opens an additional window. It displays the screen content of your host system. The Remote Console will behave exactly the same way as if you were sitting directly in front of the remote system. That means keyboard and mouse can be used in the usual way. However, be aware of the fact that the remote system will react to keyboard and mouse actions with a slightly delay. The delay depends on the bandwidth of the line, which you use to connect to the BI080135/BI160135.

With respect to the keyboard, the very exact remote representation might lead to some confusion as your local keyboard changes its keyboard layout according to the remote host system. If you use a German administration system, and your host system uses a US English keyboard layout, for instance, special keys on the German keyboard will not work as expected. Instead, the keys will result in their US English counterpart. You can avoid such problems by adjusting the keyboard of your remote system to the same mapping as your local one.

The Remote Console window will always try to show the remote screen with its optimal size. It will adapt its size to the remote screen. However, you can always resize the Remote Console window in your local window system as usual.

Warning

The Remote Console window on your local window system is just one window among others. In order to make keyboard and mouse work, your Remote Console window must have the local input focus.

5.5.1 Remote Console Control Bar

The upper part of the Remote Console window contains a control bar. You can view the state of the Remote Console and adjust the local Remote Console settings by clicking the options. A description for each options is listed as below:

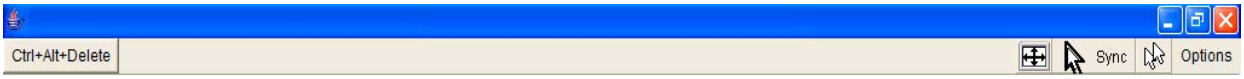
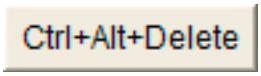


Figure 5-6. Remote Console Control Bar

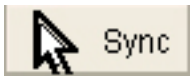


Ctrl+Alt+Delete

Special button key to send the "Control Alt Delete" key combination to the remote system (see also Chapter 6 for defining new button keys).

Auto Adjust button

If the video display quality is bad or distorted, press this button and wait a few seconds. BI080135/BI160135 will adjust automatically to get the best video quality.

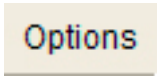


Sync mouse I

Activates the mouse synchronization process. Choose this option to synchronize the local and the remote mouse cursor. This is necessary especially when using accelerated mouse settings on the host system. In general, there is no need to change mouse settings on the host.

Single/Double mouse mode

Switches between the Single Mouse Mode (where only the remote mouse pointer is visible) and the Double Mouse Mode (where remote and local mouse pointers are visible and need to be synchronized). Single mouse mode is only available if using SUN JVM 1.4 or higher.



Options

To open the Options menu, click on the button "Options".

Figure 5-7. Remote Console Options Menu

A short description of the options follows.

- **Monitor Only**

  Toggles the "Monitor Only" on or off. If set to on, remote console interaction is disabled. Only monitoring is available.

- **Exclusive Access**

A user with the appropriate permission can close the Remote Console connections of all other users. No users can open the Remote Console until this user disables the exclusive access, or logs off.

A change in the access mode is visible in the status line (see Figure 5-8).

Figure 5-8. Remote Console Exclusive Mode

• Scaling

Allow you to scale down the Remote Console. You can still use both mouse and keyboard, however the scaling algorithm will not preserve all display details.

Figure 5-9. Remote Console Options Menu:Scaling

• Mouse Handling

The submenu for mouse handling offers two options for synchronizing the local and the remote mouse cursor.

Fast Sync -The fast synchronization is used to correct a temporary, but fixed skew.

Intelligent Sync -
Use this option if the fast sync does not work or the mouse settings have been changed on the host system.

Warning

Intelligent Sync takes more time than Fast Sync and requires a correctly adjusted picture. Use the auto adjustment function or the manual correction in the Video Settings panel to setup the picture.

- **Local Cursor**

  Offers a list of different cursor shapes to choose from for the local mouse pointer. The selected shape will be saved for the current user and activated the next time this user opens the Remote Console. The number of available shapes depends on the Java Virtual Machine; a version of 1.2 or higher offers the full list.

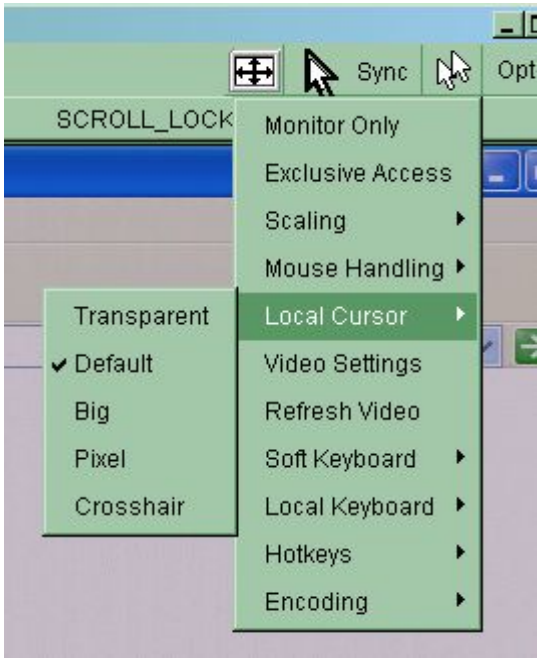


Figure 5-10. Remote Console Options Menu:Cursor

- **Video Settings**

  Opens a panel for changing the BI080135/BI160135 video settings. BI080135/BI160135 features two different dialogs, which influence the video settings.

  Video Settings through the HTML-Frontend

  To enable local video port, select this option. This option decides if the local video output of BI080135/BI160135 is active and passing through the incoming signal from the host system.

  The option Noise Filter defines how BI080135/BI160135 reacts to small changes in the video input signal. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if display content is not really changing

(depending on the quality of the video input signal). All in all the default setting should be suitable for most situations.

Video Settings through the remote console

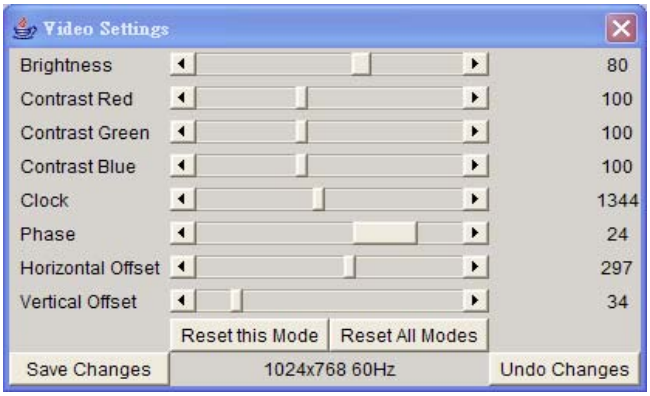


Figure 5-11. Video Settings Panel

Brightness

Controls the brightness of the picture Contrast

Controls the contrast of the picture

Clock

Defines the horizontal frequency for a video line and depends on the video mode. Different video card types may require different values here. The default settings in conjuction with the auto adjustment procedure should be adequate for all common configurations. If the picture quality is still bad after auto adjustment you may try to change this setting together with the sampling phase to achieve a better quality.

Phase

Defines the phase for video sampling, used to control the display quality together with the setting for sampling clock.

Horizontal Position

Use the left and right buttons to move the picture in horizontal direction while this option is selected.

Vertical Position

Use the left and right buttons to move the picture in vertical direction while this option is selected.

Reset this Mode

Reset clock, phase, and Horizontal/Vertical offset settings to the factory-made defaults.

Reset all Modes

Reset all settings to the factory-made defaults.

Save changes

Save changes permanently

Undo Changes

Restore last settings

• **Soft Keyboard**

Figure 5-12. Soft Keyboard

Opens up the Menu for the Soft-Keyboard.

- Show

  Pops up the Soft-Keyboard. The Soft-Keyboard is necessary in case your host system runs a completely different language and country mapping than your administration machine.

- Mapping

  Used for choosing the according language and country mapping of the Soft-Keyboard.

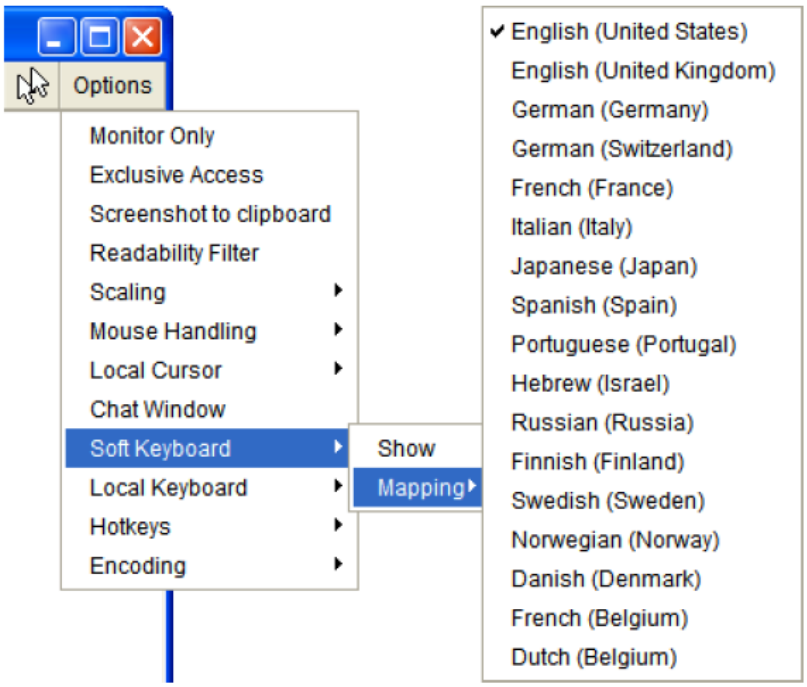


Figure 5-13. Soft Keyboard Mapping

- **Local Keyboard**

  Used to change the language mapping of your browser machine running the Remote Console Applet. Normally, the applet determines the correct value automatically. However, depending on your particular JVM and your browser settings this is not always possible. A typical example is a German localized system that uses an US-English keyboard mapping. In this case you have to change the Local Keyboard setting to the right language, manually.

- **Hotkeys**

  Opens a list of hotkeys defined before. Choose one entry, the command will be sent to the host system.

  A confirmation dialog can be added that will be displayed before sending the selected command to the remote host. Select "OK" to perform the command on the remote host.

Figure 5-14. Remote Console Confirmation Dialog

- **Encoding**

  These options are used to adjust the encoding level in terms of compression and color depth. They are only available unless "Transmission Encoding" is determined automatically (see the Section called *Transmission Encoding* in Chapter 6).

- **Compression Level:**

  you may select a value between 1 and 9 for the desired compression level with level 1 enabling the fastest compression and level 9 the best compression.

  The most suitable compression level should always be seen as a compromise between the network bandwidth that is available, on your video picture to be transferred, and on the number of changes between two single video pictures.

  We recommend to use a higher compression level if the network bandwidth is low. The higher the compression level the more time is needed to pack and unpack the video data on either side of the connection. The compression quality depends on the video picture itself, e.g. the number of the colors or the diversity of pixels.

  The lower the compression quality, the more data have to be sent and the longer it may take to transfer the whole video picture.

  If level 0 is chosen the video compression is disabled, completely.

  The option "Video Optimized" has its advantages if transferring high-quality motion pictures. In this case the video compression is disabled, completely and all video data is transferred via network as full-quality video snippets. Therefore, a high amount of bandwidth is required to ensure the quality of the video picture.

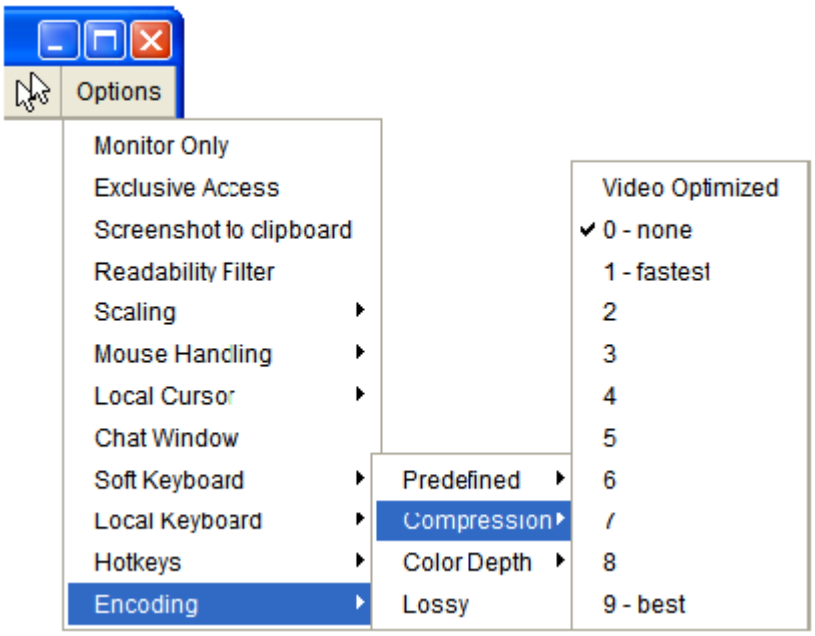


Figure 5-15 Encoding Compression

The next two options allow you to set the compression level to a predefined level OR to set a level for "lossy" compression. This compresses well, but leads to a degradation in image quality.

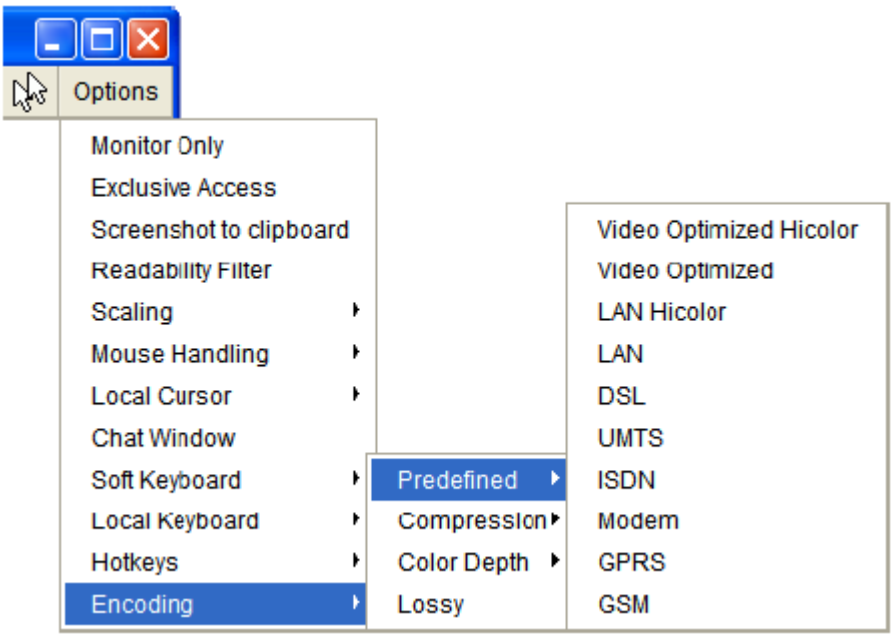


Figure 5-16 Predefined Compression

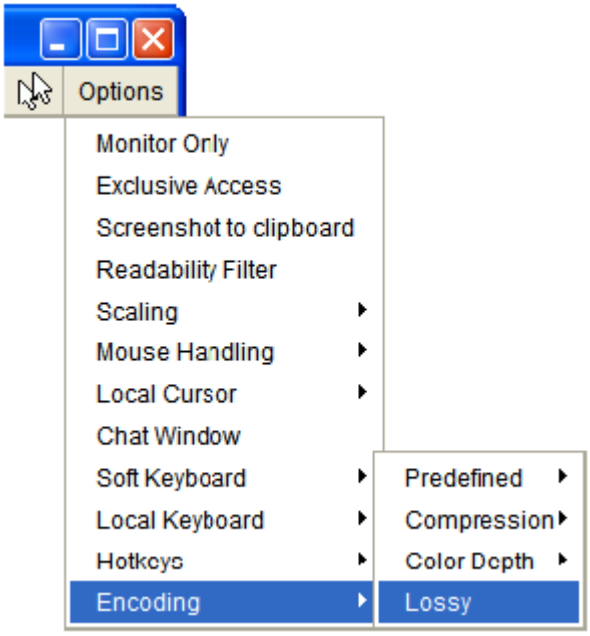


Figure 5-17 Lossy Compression

- **Color Depth:**

  set the desired color depth. You may select between 8 or 16 bit for Video Optimized/compression level 0, or between 1 and 8 bit for compression level 1 to 9. The higher the color depth, the more video information has to be captured and to be transferred.

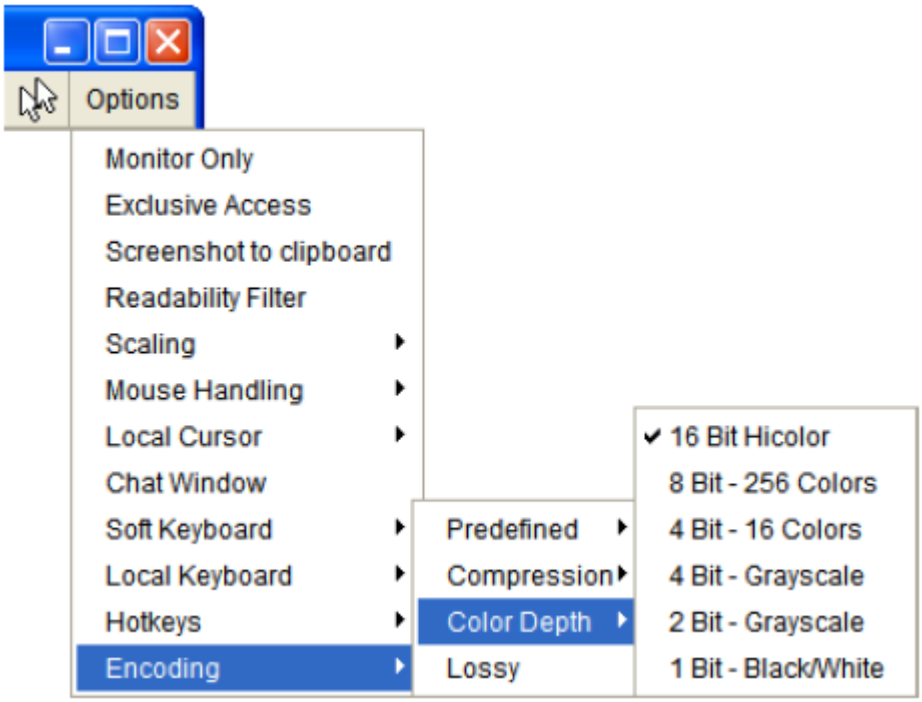


Figure 5-18 Encoding Color depth

Note: If displaying motion pictures on a connection with low speed you may achieve an improvement regarding the video transfer rate by lowering the color depth and disabling the option "Video Optimized". As a general result, the data rate is reduced (less bits per color). Furthermore, the OPMA module will not have to do any video compression. In total, this will lead to less transfer time of the motion picture.

5.5.2 Remote Console Status Line

Status line

Shows both console and the connection state. The size of the remote screen is displayed. Figure 5-15 was captured from a Remote Console Screen with a resolution of 800x600 pixels. The value in brackets describes the connection to the Remote Console. "Norm" means a standard connection without encryption, "SSL" indicates means a secure connection.

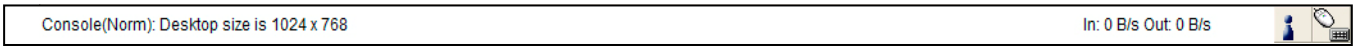


Figure 5-19. Status line

Furthermore, both the incoming ("In:") and the outgoing ("Out:") network traffic are visible (in kb/s). If compressed encoding is enabled, a value in brackets displays the compressed transfer rate.

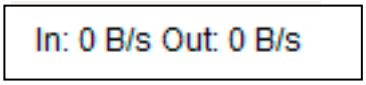


Figure 5-20. Status line transfer rate

For more information about Monitor Only and Exclusive Access settings, see the according sections

6. Menu Options 6.1

6.1 Remote Control

6.1.1 KVM Console

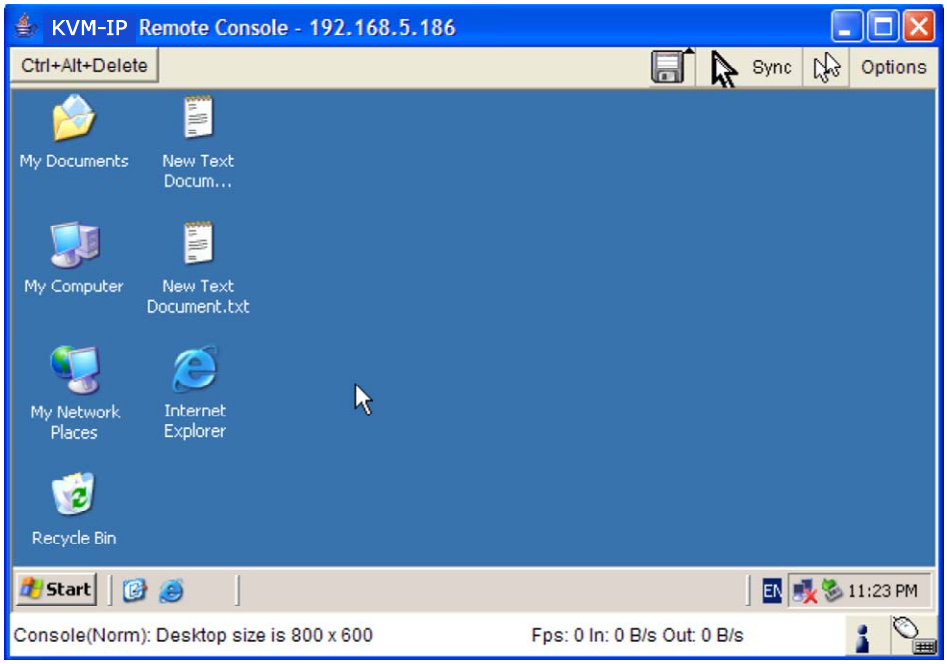


Figure 6-1. KVM Console

To open the KVM console, either clicks on the menu entry on the left, or on the console picture on the right. To refresh the picture, click on the button "Refresh".

6.1.2 Telnet Console

Figure 6-2. Telnet Console

The BI080135/BI160135 firmware features a Telnet server that enables a user to connect via a standard Telnet client. In case the Telnet program is using a VT 100, VT 102 or VT 220 terminal or an according emulation, it is even possible to perform a console redirection as long as the BI080135/BI160135 host machine is using a text mode screen resolution.

Connecting to the BI080135/BI160135 is done as usual and as required by the Telnet client, for instance in a UNIX shell:

telnet 192.168.0.70

Replace the IP address by the one that is actually assigned to the BI080135/BI160135. This will prompt for username and password in order to log into the device. The credentials that need to be entered for authentication are identical to those of the web interface. That means, the user management of the Telnet interface is entirely controlled with the according functions of the web interface.

Once you have successfully logged into the BI080135/BI160135 a command line will be presented and you can enter according management commands.

In general, the Telnet interface supports two operation modes: the command line mode and the terminal mode. The command line mode is used to control or display some parameters. In terminal mode the pass-through access to serial port 1 is activated (if the serial settings were made accordingly). All inputs are redirected to the device on serial port 1 and its answers are displayed on the Telnet interface.

The following list shows the according command mode command syntax and their usage.

Help Displays the list of possible commands

cls

Clears the screen

quit

Exits the current session and disconnects from the client

version

Displays the release information

terminal

Starts the terminal passthrough mode for serial port 1. The key sequence esc exit switches back to the command mode. The command has an optional parameter (1 or 2) to select the desired serial port for passthrough access.

6.2 Virtual Media

6.2.1 Floppy Disk

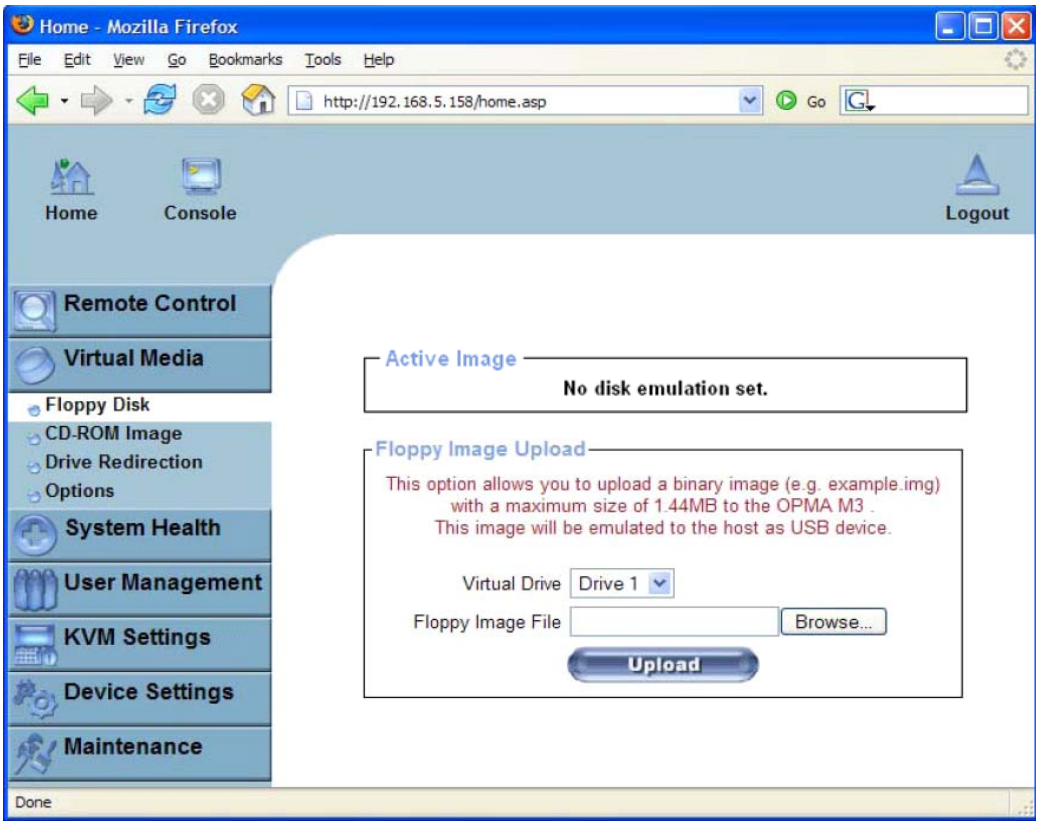
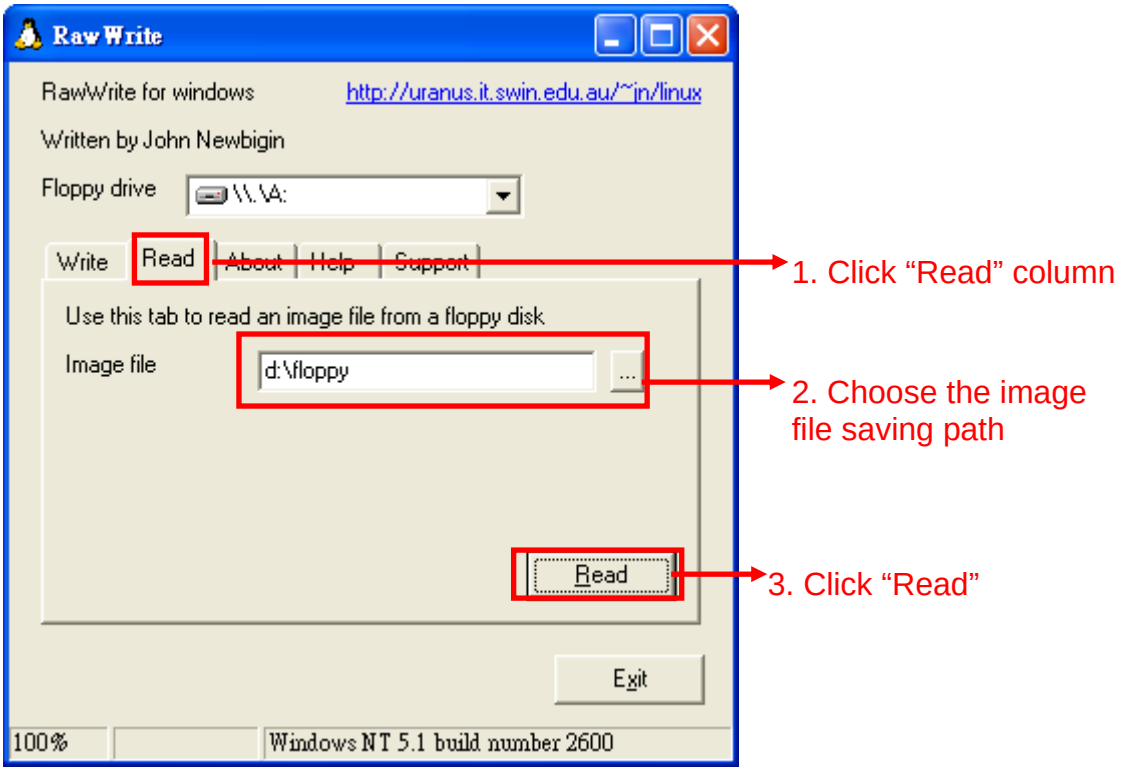


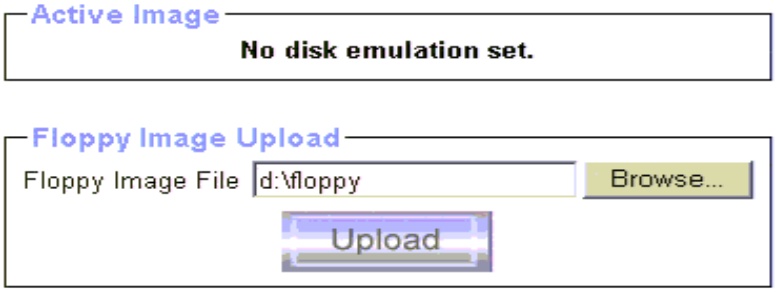
Figure 6-3. Virtual Floppy Area

1. You need to create the floppy to an image file first.
2. For this example, we use RawWrite software (or any other image-creator software) to create floppy image. Please use licensed software for this purpose.

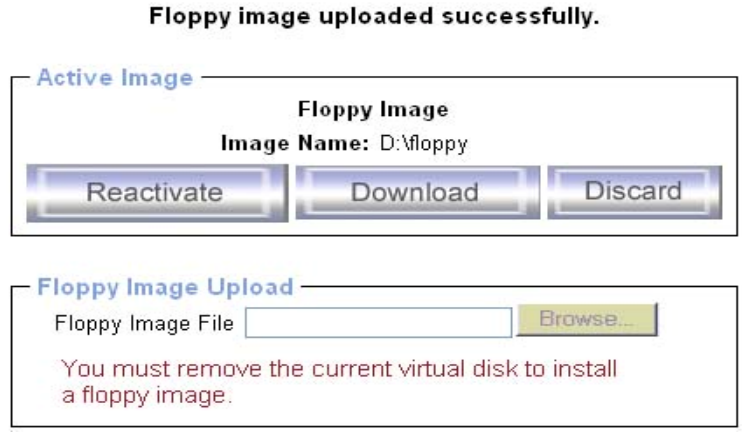


3. You can find a image file saved at desire destination after you created it with RawWrite.

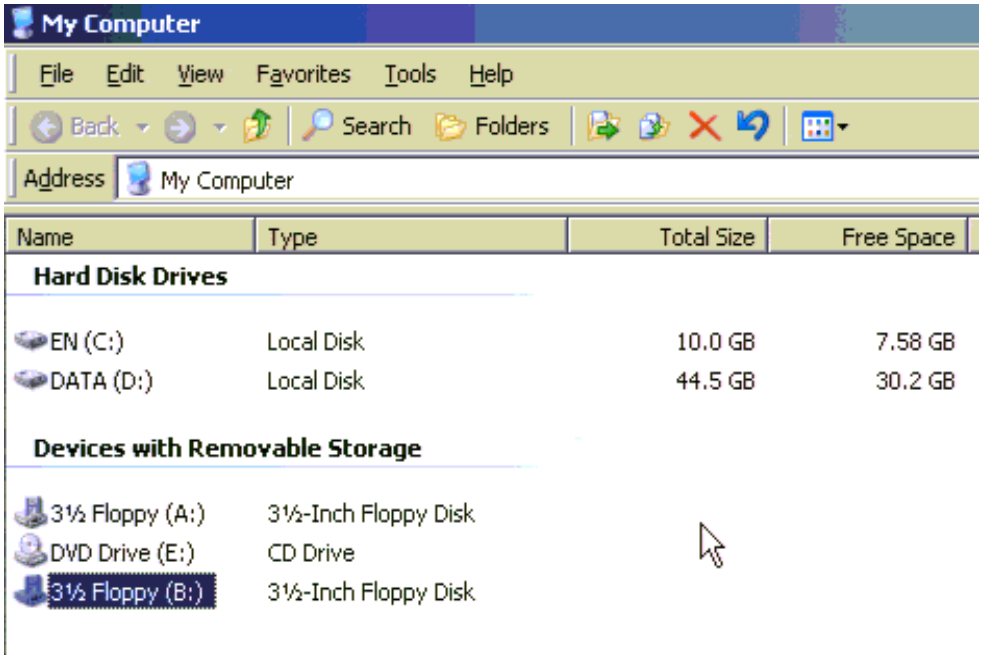
4. Open the browser to log into the BI080135/BI160135. Click **Virtual Media > Floppy Disk.** Click the Browse button to choose the image file.



5. After you uploading the image file, you will see the information below.



6. Open the remote console and you will see a virtual Floppy drive is created on the host computer that connect to BI080135/BI160135


My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer
Name Type Total Size Free Space
Hard Disk Drives
EN (C:) Local Disk 10.0 GB 7.58 GB
DATA (D:) Local Disk 44.5 GB 30.2 GB
Devices with Removable Storage
3½ Floppy (A:) 3½-Inch Floppy Disk
DVD Drive (E:) CD Drive
3½ Floppy (B:) 3½-Inch Floppy Disk

You may create a floppy image size up to 1.44Mb. This drive would be in read-only mode and would not allow you to write any information on this drive but copying only. This drive would be bootable under DOS mode if the motherboard/BIOS on the host computer supporting USB BOOTABLE function.

Notes:

1. If using other image-creator software, the output image extension file name has to be ‘img’, e.g. floppy_vir.img.

2. The uploaded image file will be kept in the onboard memory of the BI080135/BI160135 until the end of the current session, as you logged out, or initiated a reboot of the BI080135/BI160135.

6.2.2 CD ROM

Use Image on Windows Share (SAMBA)

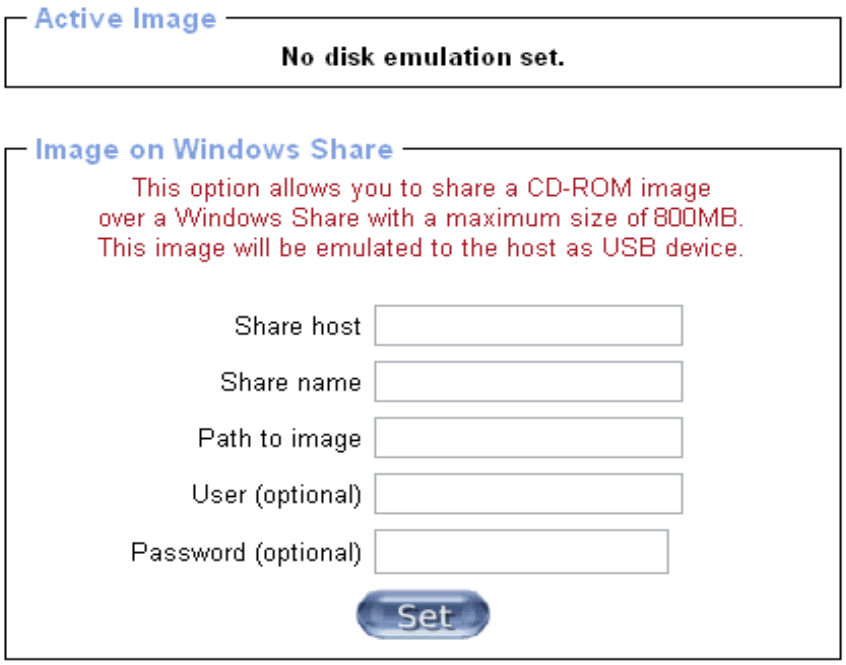

Active Image
No disk emulation set.
Image on Windows Share
This option allows you to share a CD-ROM image
over a Windows Share with a maximum size of 800MB.
This image will be emulated to the host as USB device.
Share host
Share name
Path to image
User (optional)
Password (optional)
Set

Figure 6-4. Selecting CD ROM

To include an image from a Windows share, select " CD-ROM " from the submenu.

Operation Procedures:

1. Please run Nero or any CD imaging tool to create CD-ROM ISO image.
2. Please create a folder and share this folder. (Please make sure password has to be setup with the authorized user during Sharing => Permission settings)
3. Copy the CD-ROM ISO image file to this sharing folder.
4. Please fill in the sharing information as below picture.

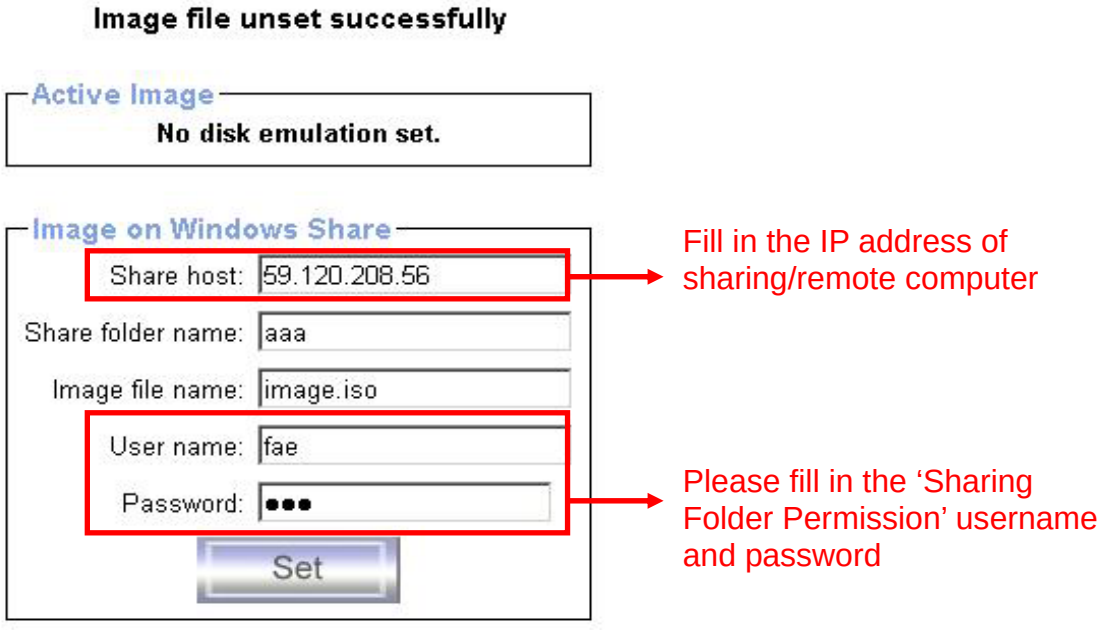
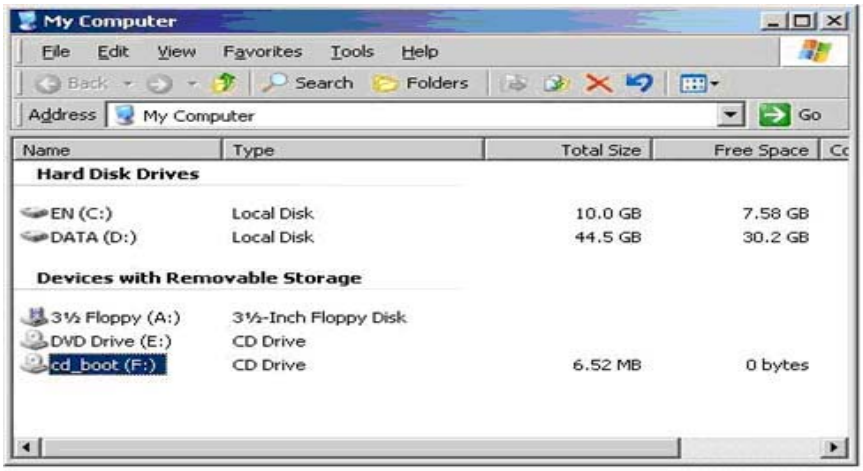


Image file unset successfully
Active Image
No disk emulation set.
Image on Windows Share
Share host: 59.120.208.56
Share folder name: aaa
Image file name: image.iso
User name: fae
Password: ●●●
Set
Fill in the IP address of sharing/remote computer
Please fill in the 'Sharing Folder Permission' username and password

5. Image file set successfully.

6. Open the remote console, you can see the virtual CD as below picture.


My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer
Go
Name Type Total Size Free Space
Hard Disk Drives
EN (C:) Local Disk 10.0 GB 7.58 GB
DATA (D:) Local Disk 44.5 GB 30.2 GB
Devices with Removable Storage
3½ Floppy (A:) 3½-Inch Floppy Disk
DVD Drive (E:) CD Drive
cd_boot (F:) CD Drive 6.52 MB 0 bytes

Note: the output image extension file name has to be ‘iso’, e.g. CD-Rom_vir.iso.
You may create an ISO image size up to 650Mb. This drive would be in read-only mode and would not allow you to write any information on this drive but copying only. This drive would be bootable under DOS mode if the motherboard/BIOS on the host computer supports USB BOOTABLE function. For emulating DVD Drive, please use **Drive Redirection** function.

Note: The above information has to be given from the point of view of BI080135/BI160135 with correct IP address and device name. Administrative permission is required as regular user may not have the right to access. Please login as a system administrator (or as “root” on UNIX systems).

The following information has to be given to mount the image properly:

Share host -- The server name or its IP address.

Share folder name -- The name of the share folder to be used.

Image file name -- The name of the image file on the share folder.

User name -- If necessary, specify the user name for the share named in advance. If unspecified, and a guest account is activated, this guest account information will be used as your login.

Password -- If necessary, specify the password for the given user name.

To register the specified file image and its location click on the button “Set”.

The specified image file is supposed to be accessible from the BI080135/BI160135. The information above has to be given from the point of view of the BI080135/BI160135. It is important to specify correct IP addresses, and device names. Otherwise, BI080135/BI160135 may not be able to access the referenced image file.

Furthermore, the specified share has to be configured correctly. Therefore, administrative permissions are required. As a regular user you may not have these permissions. You should either login as a system administrator (or as “root” on UNIX systems), or ask your system administrator for help to complete this task.

MS Windows

Open the Explorer, navigate to the directory (or share), and press the right mouse button to open the context menu.

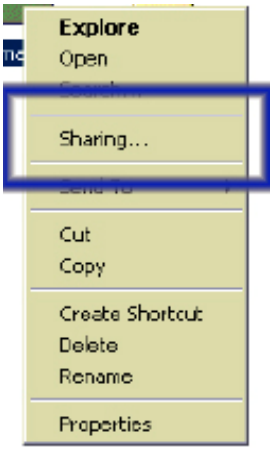


Figure 6-1 Explorer context menu

Select “Sharing” to open the configuration dialog.

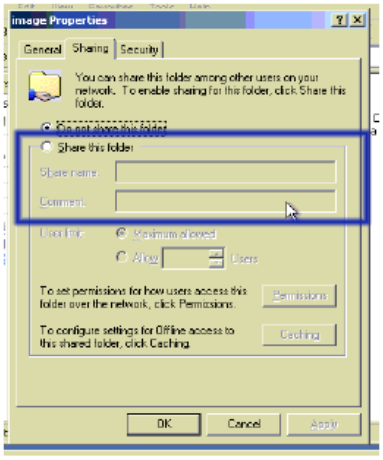


Figure 6-2 Share configuration dialog

Adjust the settings for the selected directory.

- Activate the selected directory as a share. Select “Sharing this folder”.
- Choose an appropriate name for the share. You may also add a short description for this folder (input field “Comment”).
- If necessary, adjust the permissions (button “permissions”).
- Click “OK” to set the options for this share.

UNIX and UNIX-like OS (Sun Solaris, and Linux)

If you like to access the share via SAMBA, SAMBA has to be set up properly. You may either edit the SAMBA configuration file /etc/samba/smb.conf, or use the Samba Web Administration Tool (SWAT) or WebMin to set the correct parameters.

6.2.3 Drive redirection

The Drive Redirection is another possibility to use a virtual disc drive on the remote computer. With Drive Redirection you do not have to use an image file but may work with a drive from your local computer on the remote machine. The drive is hereby shared over a TCP network connection. Devices such as floppy drives, hard discs, CD ROMs and other removable devices like USB sticks can be redirected. It is even possible to enable a write support so that for the remote machine it is possible to write data to your local disc.

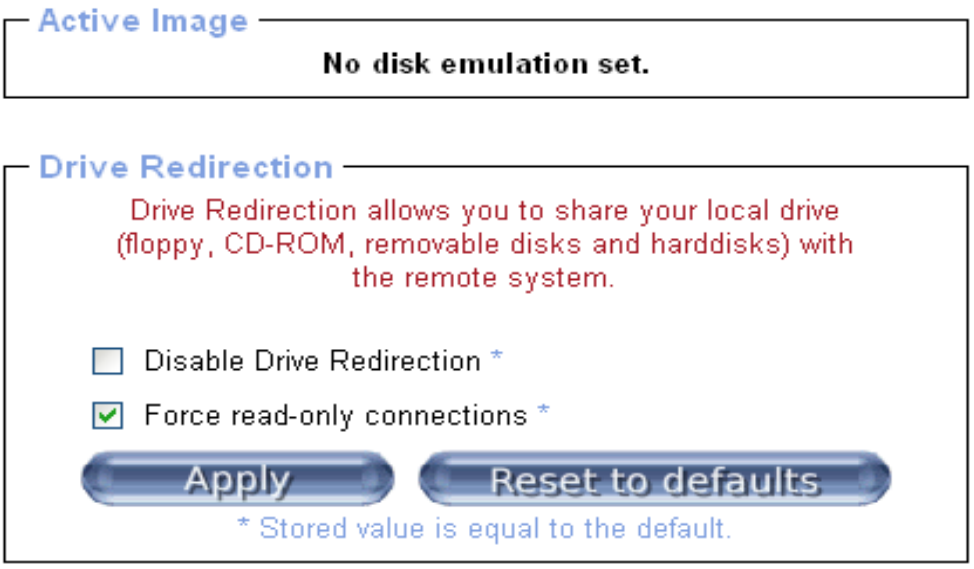

Active Image
No disk emulation set.
Drive Redirection
Drive Redirection allows you to share your local drive (floppy, CD-ROM, removable disks and harddisks) with the remote system.
Disable Drive Redirection *
Force read-only connections *
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 6-3 Options of Drive Redirection

Please note that Drive Redirection works on a level which is far below the operating system. That means that neither the local nor the remote operating system is aware that the drive is currently redirected, actually. This may lead to inconsistent data as soon as one of the operating systems (either from the local machine, or from the remote host) is writing data on the device. If write support is enabled the remote computer might damage the data and the file system on the redirected device. On the other hand, if the local operating system writes data to the redirected device the drive cache of the operating system of the remote host might contain older data. This may confuse the remote host's operating system. We recommend to use the Drive Redirection with care, especially the write support.

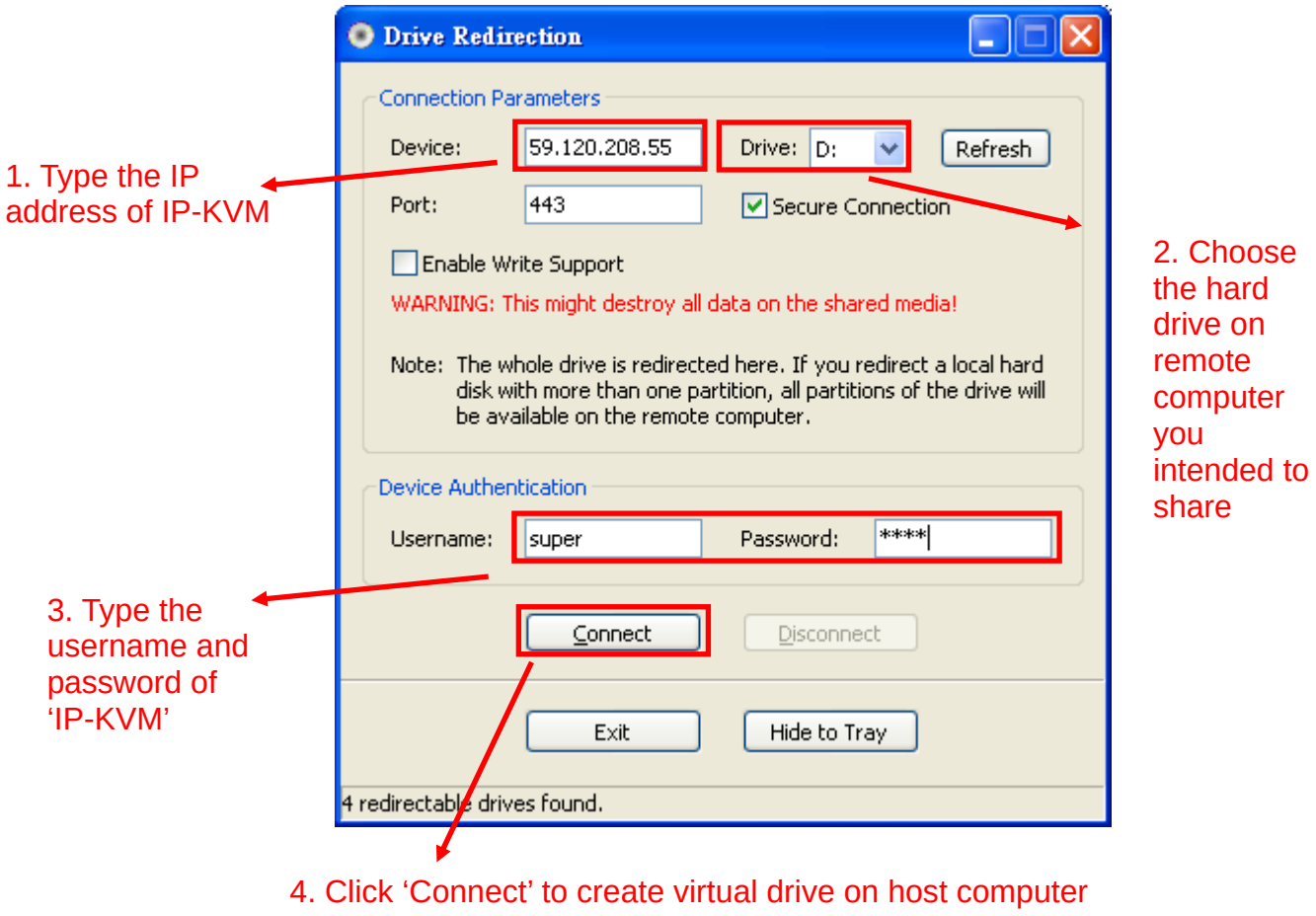
Disable Drive Redirection
If enabled the Drive Redirection is switched off.

Force read-only connections
If enabled the Write Support for the Drive Redirection is switched off. It is not possible to write on a redirected device.

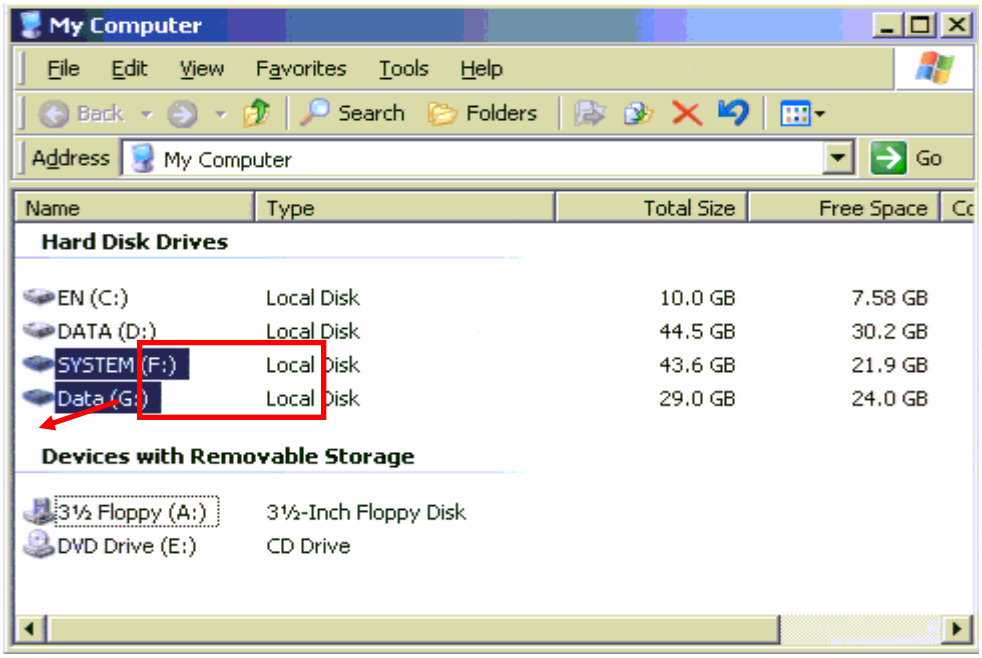
Click **Apply** to submit your changes.

Operation Procedures:

1. Please install Drive Redirection Software on remote computer first then run Drive Rediection application and fill in information accordingly:


1. Type the IP address of IP-KVM
Drive Redirection
Connection Parameters
Device:
59.120.208.55
Drive:
D:
Refresh
Port:
443
Secure Connection
Enable Write Support
WARNING: This might destroy all data on the shared media!
Note: The whole drive is redirected here. If you redirect a local hard disk with more than one partition, all partitions of the drive will be available on the remote computer.
2. Choose the hard drive on remote computer you intended to share
Device Authentication
Username:
super
Password:
****
3. Type the username and password of 'IP-KVM'
Connect
Disconnect
Exit
Hide to Tray
4 redirectable drives found.
4. Click 'Connect' to create virtual drive on host computer

2. Open the remote and you can see the virtual hard drive as below picture.


My Computer
File Edit View Favorites Tools Help
Back Search Folders
Address My Computer
Go
Name
Type
Total Size
Free Space
Hard Disk Drives
EN (C:) Local Disk 10.0 GB 7.58 GB
DATA (D:) Local Disk 44.5 GB 30.2 GB
SYSTEM (F:) Local Disk 43.6 GB 21.9 GB
Data (G:) Local Disk 29.0 GB 24.0 GB
Devices with Removable Storage
3½ Floppy (A:) 3½-Inch Floppy Disk
DVD Drive (E:) CD Drive
Virtual Drive has been created

Please note that Virtual Drive creation is by Device manner not by Partition. Which means it looks for I/O in BIOS and sends the corresponding signal to host computer. This way, you are sending the entire hard drive (may consist of 'X' numbers of partitions) and emulate whatever number of partitions on host computer. You may also emulate a DVD-Drive with the same procedure. However, this DVD-Drive **Does NOT** support Bootable function like

Floppy and CD-Rom emulation.

There are two methods of Drive Redirections:

1. External Drive Redirection Utility
2. Built-in Java Drive Redirection function in Remote Console

6.2.3.1 Driver Redirection Utility Installation

Please follow the Drive Redirection Setup Wizard step by step to install the driver from the attached CD ROM.

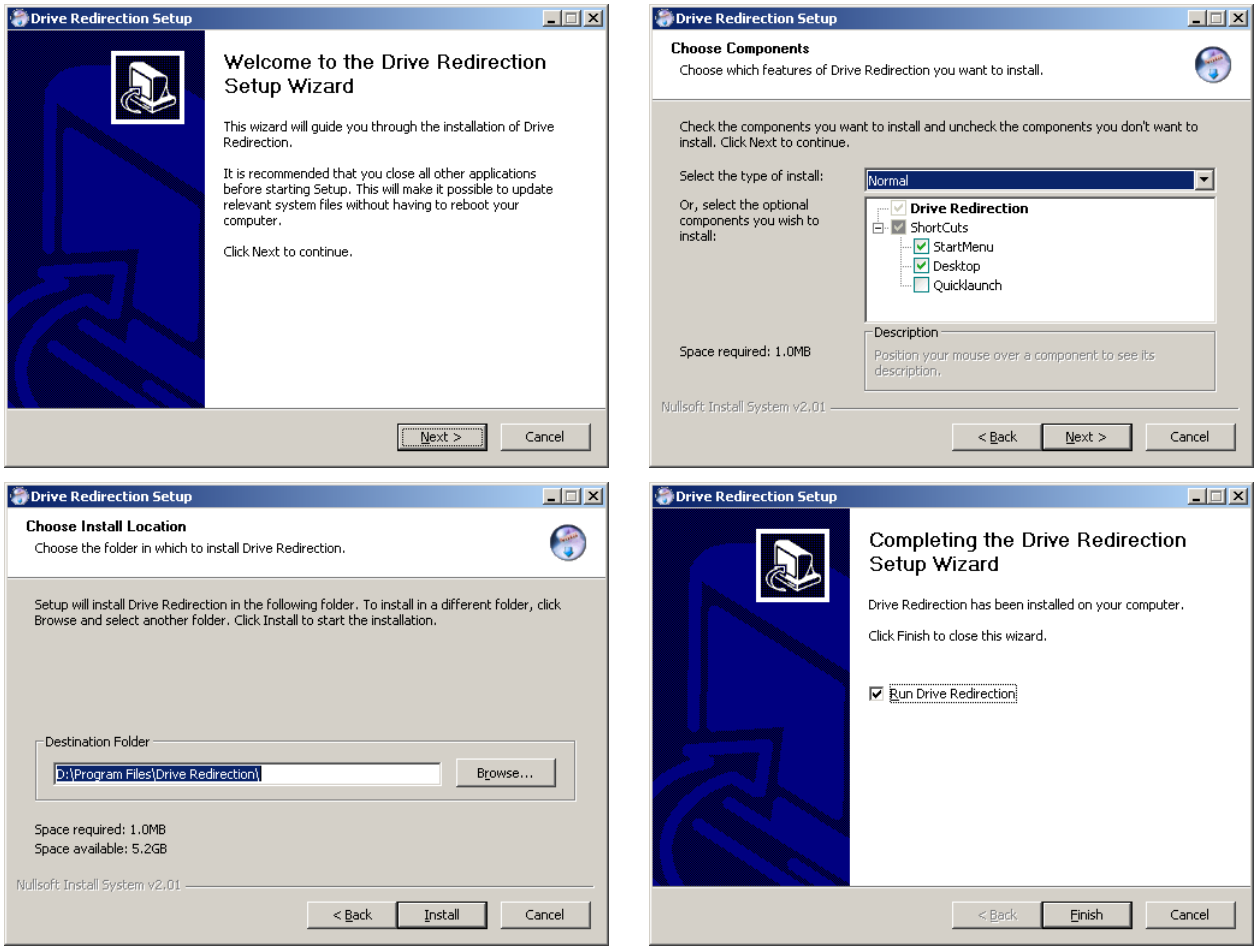

Drive Redirection Setup
Welcome to the Drive Redirection Setup Wizard
This wizard will guide you through the installation of Drive Redirection.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
Next >
Cancel
Drive Redirection Setup
Choose Components
Choose which features of Drive Redirection you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select the type of install:
Normal
Or, select the optional components you wish to install:
Drive Redirection
ShortCuts
StartMenu
Desktop
Quicklaunch
Description
Position your mouse over a component to see its description.
Space required: 1.0MB
Nullsoft Install System v2.01
< Back
Next >
Cancel
Drive Redirection Setup
Choose Install Location
Choose the folder in which to install Drive Redirection.
Setup will install Drive Redirection in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
D:\Program Files\Drive Redirection\
Browse...
Space required: 1.0MB
Space available: 5.2GB
Nullsoft Install System v2.01
< Back
Install
Cancel
Drive Redirection Setup
Completing the Drive Redirection Setup Wizard
Drive Redirection has been installed on your computer.
Click Finish to close this wizard.
Run Drive Redirection
< Back
Finish
Cancel

Figure 6-4 Drive Redirection Setup

Drive Redirection Settings

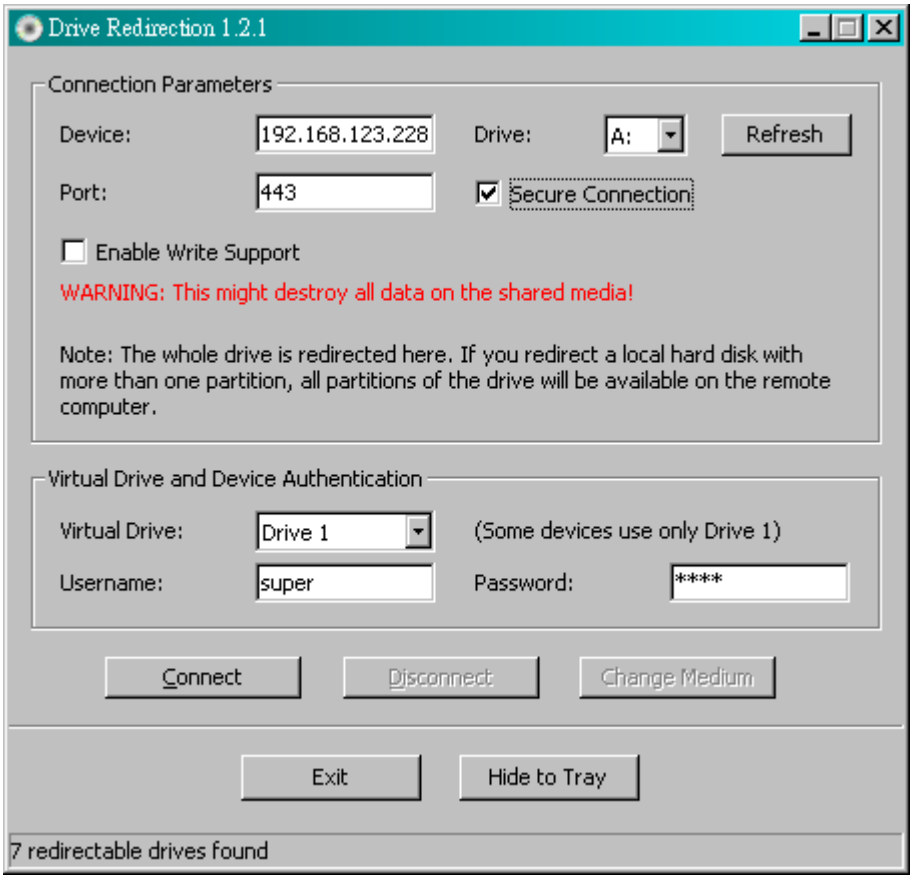


Figure 6-5 Drive Redirection dialog

Drive Redirection Utility:

Device

This is the address (either the DNS name or the IP address) of the BI080135/BI160135 you would like to connect to.

Drive

The local drive you want to share with the remote computer, which could be Floppy disc, CD-ROMs, USB-Sticks and hard drives.

Port

This is the network port. By default, BI080135/BI160135 uses the remote console port (#443) here. You may change this value if you have changed the remote console port in your BI080135/BI160135 network settings.

Secure Connection

Enable this box to establish a secure connection via SSL. This will maximize the security but may reduce the connection speed.

Select the drive you would like to redirect. All available devices (drive letters) are shown here. Please note that the whole drive is shared with the remote computer, not only one partition. If you have a hard disc with more than one partition all drive letters that belong to this disc will be redirected. The Refresh button may be used to regenerate the list of drive letters, especially for an USB stick.

Warning

Please be cautious that if “Allow Write Support” is selected, all data on the shred media might be destroyed.

Write Support
This feature may be enabled here. Write support means that the remote computer is allowed to write on your local drive. As you can imagine, this is very dangerous. If both the remote and the local system try to write data on the same device, this will certainly destroy the file system on the drive. Please use this only when you exactly know what you are doing.

Device Authentication
The factory default Username is “super” and the default Password is “pass”.
Click **Connect** to redirect drive

Warning

1. Drive Redirection is only possible with Windows 2000 or above versions.
2. The Drive Redirection works on a low SCSI level and the SCSI protocol cannot recognize partitions; therefore the whole drive selected will be shared instead of any particular partition.
3. While connecting to a legacy KVM switch, please select PS/2 mouse for **Keyboard/Mouse setting** from webpage. Otherwise you will not be able to use Hot-key.

Connect/Disconnect

To establish the drive redirection please press the **Connect** button once. If all the settings are correct, the status bar displays that the connection has been established, the Connect button is disabled and the Disconnect button is enabled.

On an error, the status line shows the error message. The drive redirection software tries to lock the local drive before it is redirected. That means that it tries to prevent the local operating system from accessing the drive as long as it is redirected. This may also fail, especially if a file on the drive is currently open. In the case of a locking failure, you will be prompted if you want to establish the connection anyhow. This should not be a serious problem when the note above is respected. If the write support is enabled, a drive which is not locked might be damaged by the Drive Redirection.

With the **Disconnect** button, a connection via Drive Redirection connection is stopped.

Exit/Hide

If the **Exit** button is pressed, the Drive Redirection software is closed. If a Drive Redirection
connection is active, the connection will be closed before the application terminates.

Using the Hide to Tray button the application is hidden, but not terminated completely. That means that an active connection will be kept active until it is closed explicitly. You can access the software by its tray icon. The tray icon also shows whether a connection is established or not. A double click on the icon shows the application window, or with a right click you may access a small menu

6.2.3.2 Built-in Java Drive Redirection

1. Run Remote Control > KVM Console.
2. Click “Floppy” icon

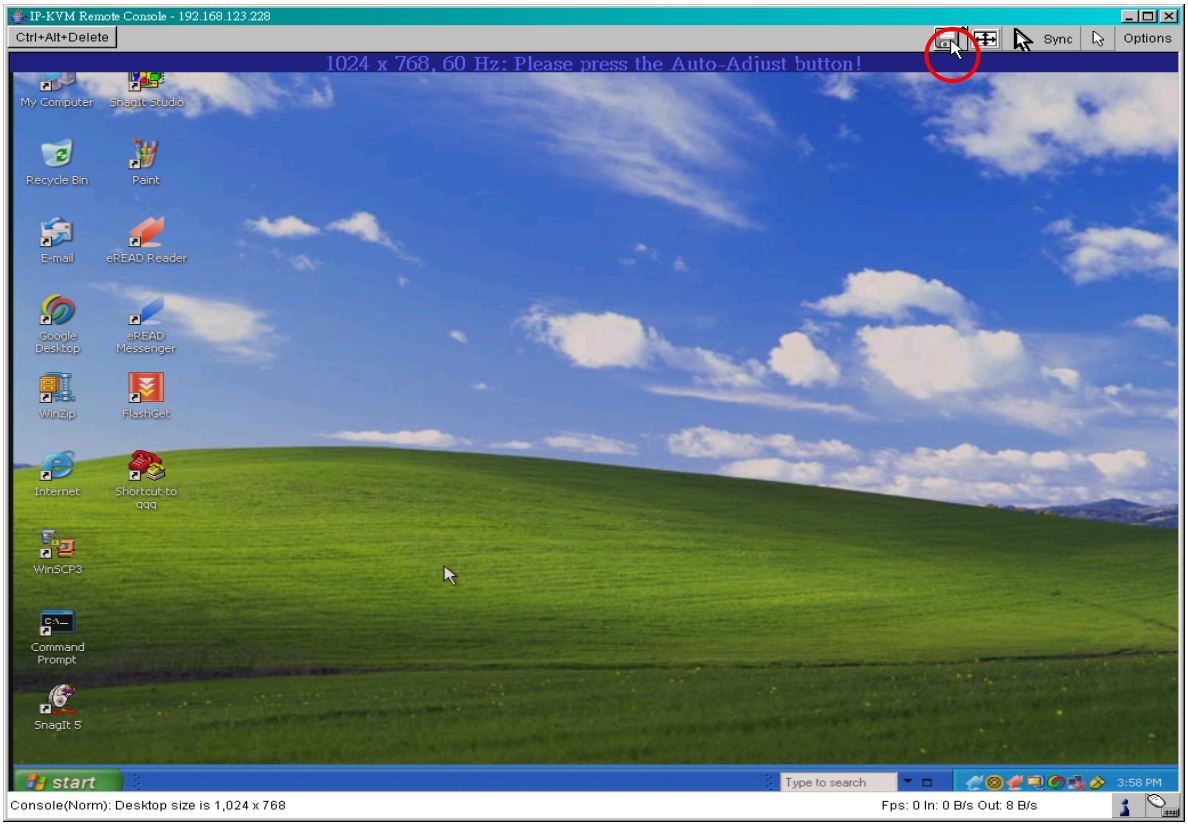
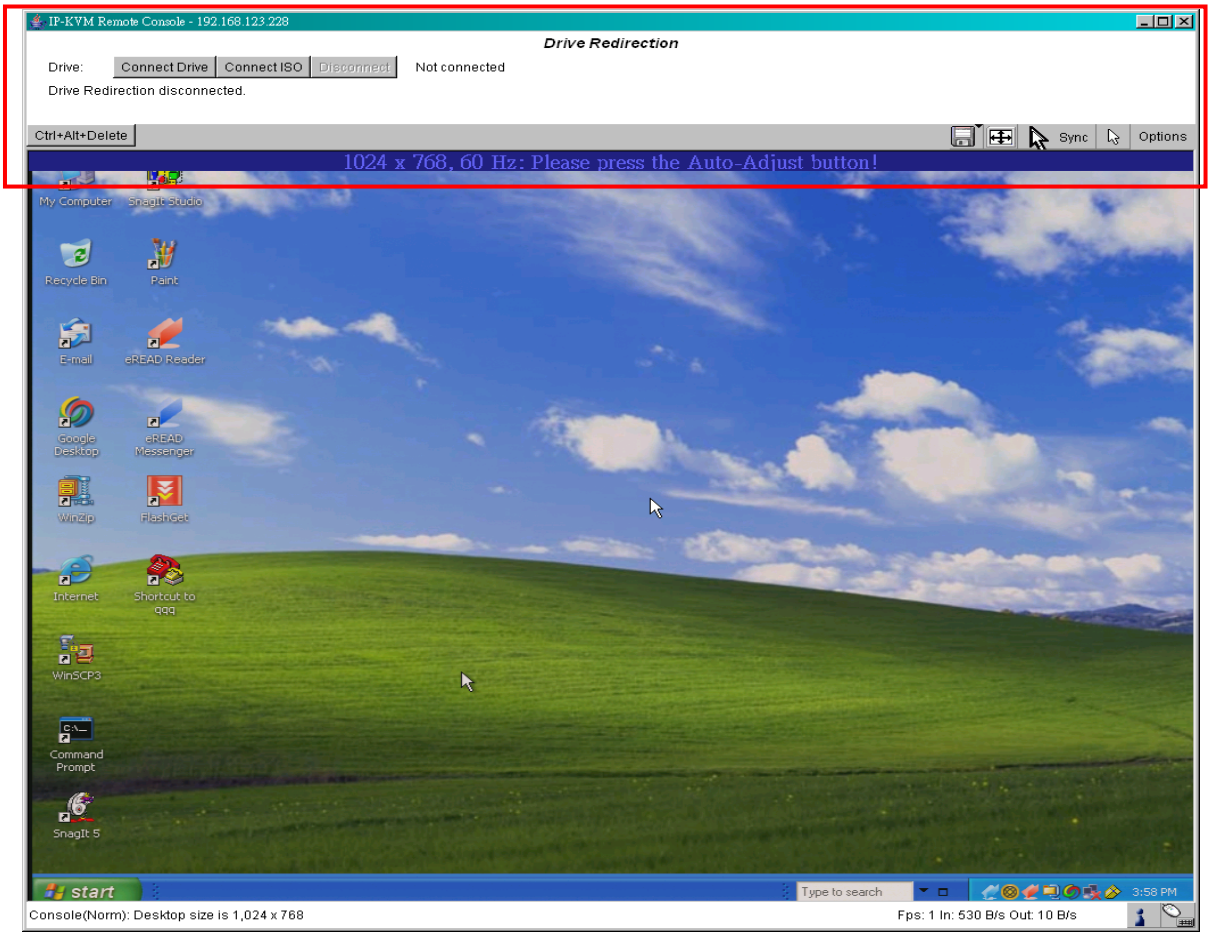
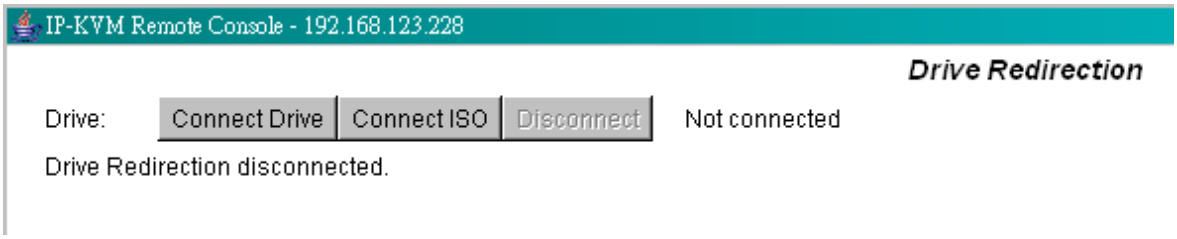


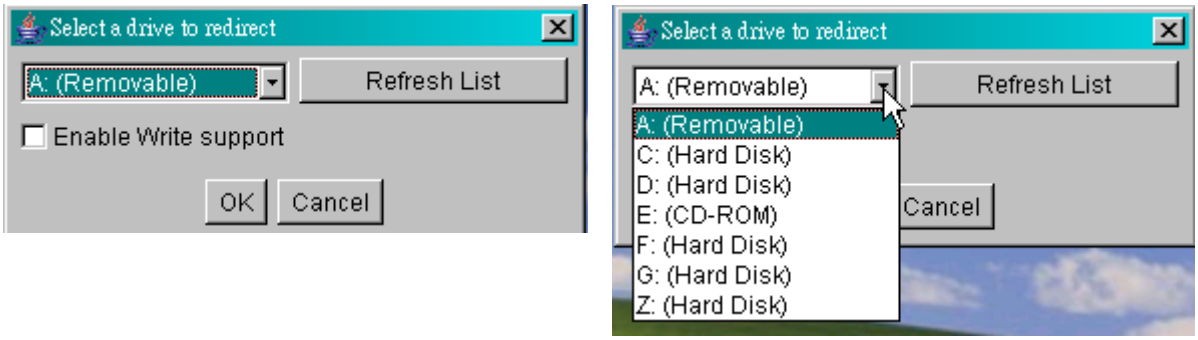
Figure 6-6 Built-in Java Drive Redirection



3. Click **Connect Drive** or **Connect ISO**



4. Select a drive to redirect (if Connect Drive)



5. Select a ISO image to redirect (if Connect ISO)

6.2.4 Options

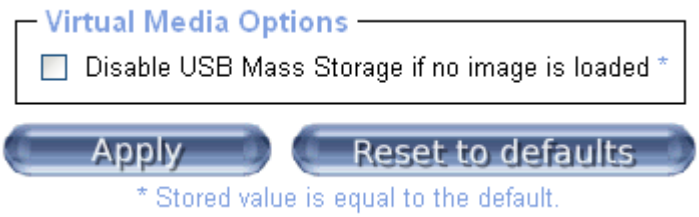

Virtual Media Options
Disable USB Mass Storage if no image is loaded *
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 6-7 USB mass storage option

Set this option to disable the mass storage emulation (and hide the virtual drive) if no image file is currently loaded. If unset, and no file image will be found it may happen that the host system will hang on boot due to changes in the boot order, or the boot manager (LILO, GRUB). This case was reported for some Windows versions (2000, XP), other OS might not be fully excluded. This behavior depends on the BIOS version used in that machine.

To set this option, press the button “Apply”.

6.2.4.1 Floppy Images

UNIX and UNIX-like OS

To create an image file, make use of “dd”. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, and Linux).

To create a floppy image file, copy the contents of a floppy to a file. You can use the following command:

dd [*if=/dev/fd0*] [*of=/tmp/floppy.image*]

dd reads the entire disc from the device /dev/fd0, and saves the output in the specified output file /tmp/floppy.image. Adjust both parameters exactly to your needs (input device etc.)

MS Windows

You can use the tool “Raw Write for Windows”. It is included on the CD ROM shipped with IP-KVM.

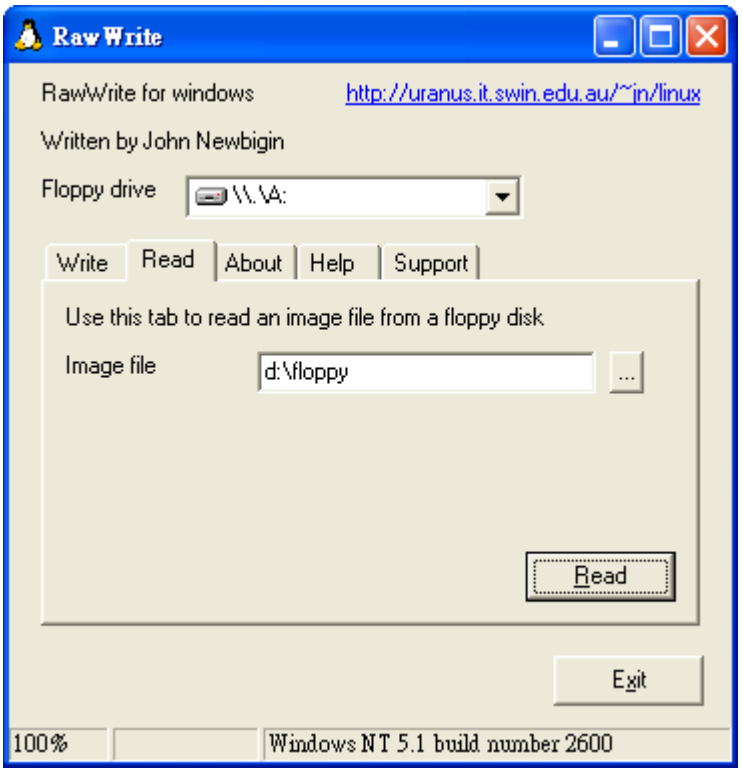


Figure 6-8 RawWrite for Windows selection dialog

From the menu, select the tab “Read”. Enter (or choose) the name of the file in which you would like to save the floppy content. Click on the button “Copy” to initiate the image creation process.

For related tools you may have a look at www.fdos.org

6.2.4.2 CD ROM/ISO Images

UNIX and UNIX-like OS

To create an image file, make use of “dd”. This is one of the original UNIX utilities and is included in every UNIX-like OS (UNIX, Sun Solaris, and Linux).

To create a CDROM image file, copy the contents of the CDROM to a file. You can use the following command:

dd [*if=/dev/cdrom*] [*of=/tmp/cdrom.image*]

dd reads the entire disc from the device /dev/cdrom, and saves the output in the specified output file /tmp/cdrom.image. Adjust both parameters exactly to your needs (input device etc.).

MS Windows

To create the image file, use your favorite CD imaging tool. Copy the whole contents of the disc into one single image file on your hard disk.

For example, with “Nero” you choose “Copy and Backup”. Then, navigate to the “Copy Disc” section. Select the CD ROM or DVD drive you would like to create an image from. Specify the filename of the image, and save the CD ROM content in that file.

Figure 6-9 Nero selection dialog

6.3 User Management

6.3.1 Change Password

Figure 6-10. Setting password

Change password of currently logged in user:

Old Password: type in current password

New Password: type in new password

Confirm New Password: re-type new password for verification

Click “Apply” to submit your changes.

6.3.2 Users And Groups

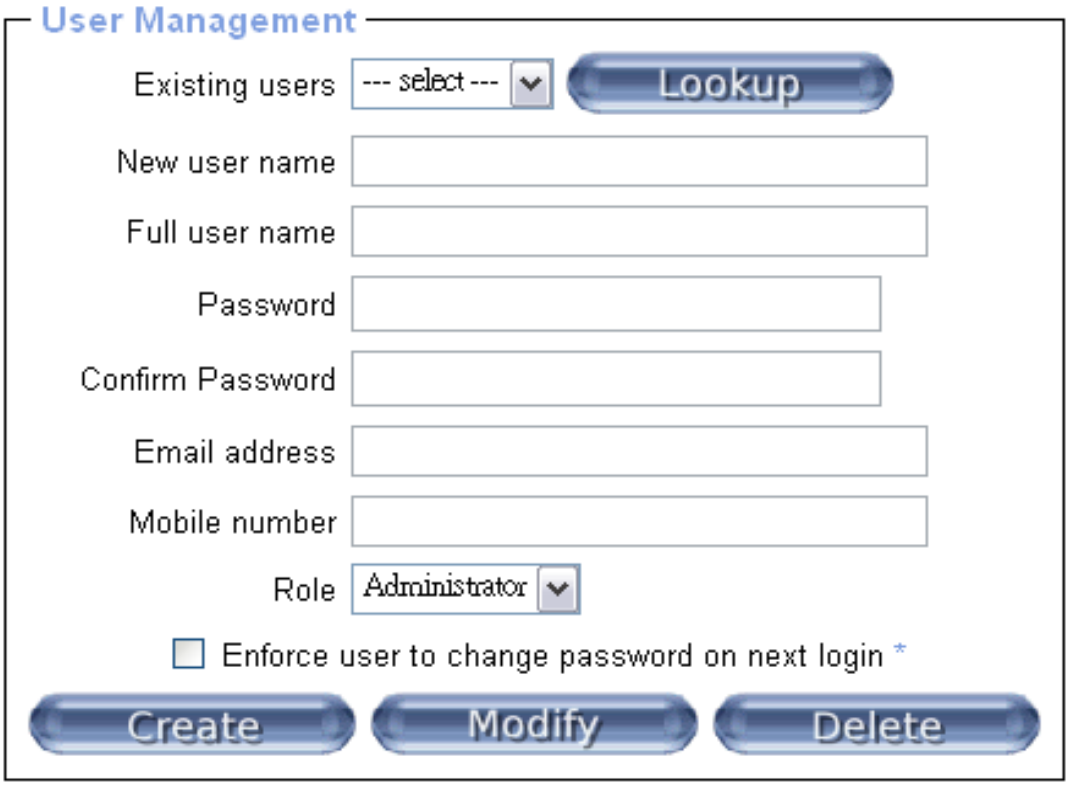


Figure 6-11. Set User

There are three kinds of levels of user accounts:

- **Super --** Has all possible rights to configure the device
- **Administrator --** Has partial rights to change configuration apart from critical settings
- **User --** Has permission to access basic function of open Remote Console

You can choose the desired level from the selection box **role**.

The BI080135/BI160135 comes with 1 pre-configured user account that has fixed permissions. The account “super” has all possible rights to configure the device and to use all functions BI080135/BI160135 offers.

Upon delivery, the account “super” has the password “pass”. Make sure to change password immediately after you have installed and on initial access of your BI080135/BI160135.

Existing users

Select an existing user for modification. Once a user has been selected, click the lookup button to see the user information.

New User name

The new user name for the selected account.

Password

The password for the login name. It must be at least three characters long.

Confirm password

Confirmation of the password above.

Email address

This is optional.

Mobile number

This information may be optionally provided.

Role

Each user can be a member of a group (named a “role”) – there kinds can be shose from: super, administrator, or an regular user.

To create an user press the button **Create**. The **Modify** button changes the displayed user settings. To delete an user press the button **Delete**.

Note:The BI080135/BI160135 is equipped with an host-independent processor and memory unit which both have a limitation in terms of the processing instructions and memory space. To guarantee an acceptable response time we recommend not to exceed the number of 15 users connected to the BI080135/BI160135 at the same time. The memory space that is available onto the BI080135/BI160135 mainly depends on the configuration and the usage of the BI080135/BI160135 (log file entries etc.). That’s why we recommend not to store more than 150 user profiles.

6.4 KVMSettings

6.4.1 User Console

The following settings are user specific. That means, the super user can customize these settings for every users separately. Changing the settings for one user does not affect the settings for the other users.

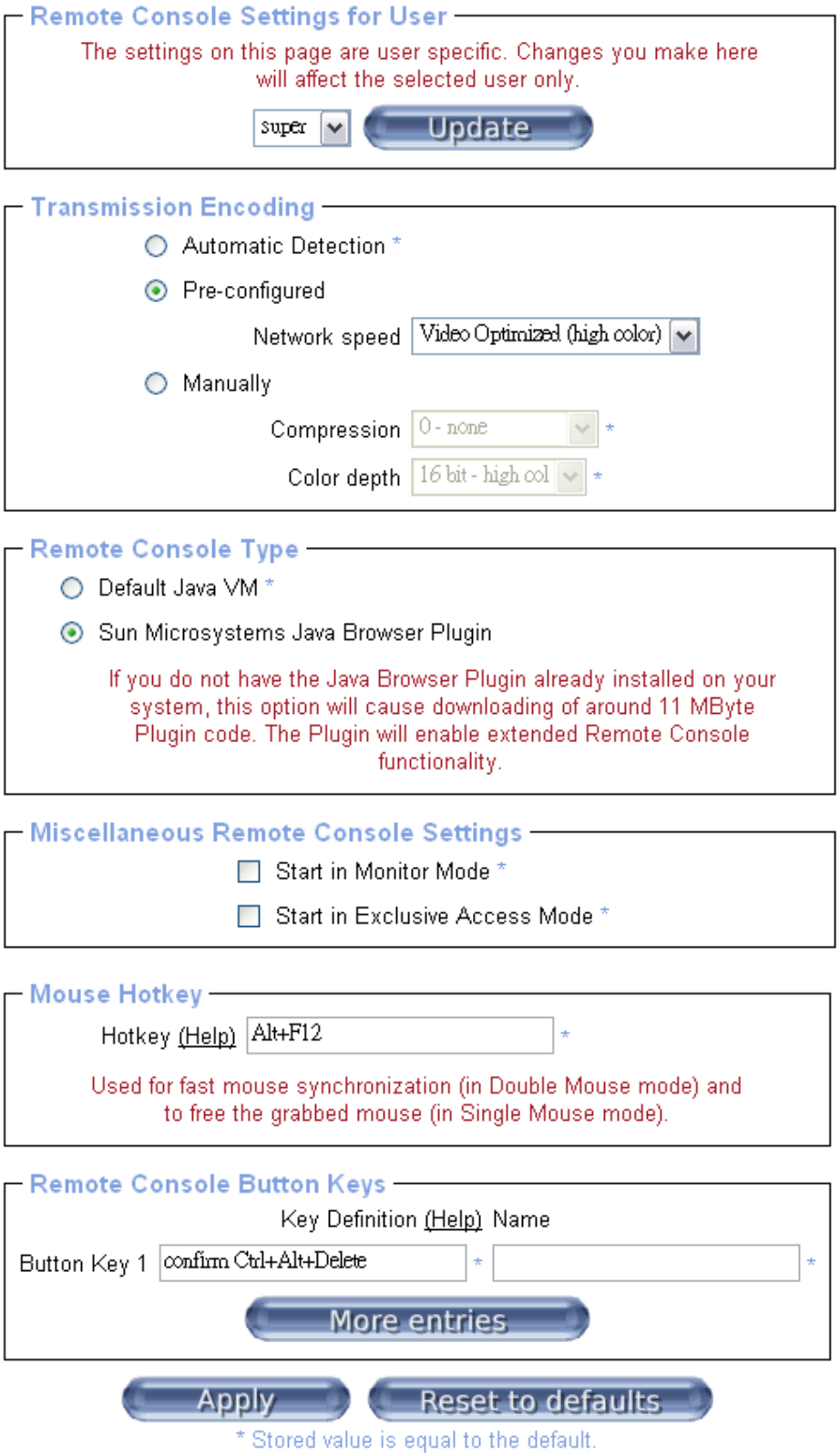

Remote Console Settings for User
The settings on this page are user specific. Changes you make here will affect the selected user only.
super
Update
Transmission Encoding
Automatic Detection *
Pre-configured
Network speed
Video Optimized (high color)
Manually
Compression
0 - none
*
Color depth
16 bit - high col
*
Remote Console Type
Default Java VM *
Sun Microsystems Java Browser Plugin
If you do not have the Java Browser Plugin already installed on your system, this option will cause downloading of around 11 MByte Plugin code. The Plugin will enable extended Remote Console functionality.
Miscellaneous Remote Console Settings
Start in Monitor Mode *
Start in Exclusive Access Mode *
Mouse Hotkey
Hotkey (Help)
Alt+F12
*
Used for fast mouse synchronization (in Double Mouse mode) and to free the grabbed mouse (in Single Mouse mode).
Remote Console Button Keys
Key Definition (Help)
Name
Button Key 1
confirm Ctrl+Alt+Delete
*
*
More entries
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 6-12. User Console Settings

User select box

This selection box displays the user ID for which the values are shown and for which the changes will take effect. You may change the settings of other users if you have the necessary access rights.

Transmission Encoding

The Transmission Encoding setting allows changing the image-encoding algorithm that is used to transmit the video data to the Remote Console window. It is possible to optimize the speed of the remote screen depending on the number of users working at the same time and the bandwidth of the connection line (Modem, ISDN, DSL, LAN, etc.).

Automatic detection

The encoding and the compression level is determined automatically from the available bandwidth and the current content of the video image.

Pre-configured

The pre-configured settings deliver the best result because of optimized adjustment of compression and colour depth for the indicated network speed.

Manually

Allows to adjust both compression rate and the colour depth individually. Depending on the selected compression rate the data stream between the BI080135/BI160135 and the Remote Console will be compressed in order to save bandwidth. Since high compression rates are very time consuming, they should not be used while several users are accessing the BI080135/BI160135 simultaneously.

The standard color depth is 16 Bit (65536 colors). The other color depths are intended for slower network connections in order to allow a faster transmission of data. Therefore compression level 0 (no compression) uses only 16 Bit color depth. At lower bandwidths only 4 Bit (16 colors) and 2 Bit (4 gray scales) are recommended for typical desktop interfaces. Photo-like pictures have best results with 4 Bit (16 gray scales). 1 Bit color depth (black/white) should only be used for extremely slow network connections.

Remote Console Type

Specifies, which Remote Console Viewer to use.

Default Java-VM

Uses the default Java Virtual Machine of your Browser. This may be the Microsoft JVM for the Internet Explorer, or the Sun JVM if it is configured this way. Use of the Sun JVM may also be forced (see below).

Sun Microsystems Java Browser Plugin

Instructs the web browser of your administration system to use the JVM of Sun Microsystems. The JVM in the browser is used to run the code for the Remote Console window, which is actually a Java Applet. If you check this box for the first

time on your administration system and the appropriate Java plug-in is not already installed on your system, it will be downloaded and installed automatically. However, in order to make the installation possible, you still need to answer the according dialogs with "yes" . The download volume is around 11 Mbytes. The advantage of downloading Sun's JVM lays in providing a stable and identical Java Virtual Machine across different platforms. The Remote Console software is optimized for this JVM versions and offers wider range of functionality when run in SUN's JVM. (Hint: If you are connected over a slow connection to the Internet you can also pre-install the JVM on your administration machine. The software is available on the CD ROM that is delivered along with the BI080135/BI160135.)

Miscellaneous Remote Console Settings

Start in Monitor Mode

Sets the initial value for the monitor mode. By default the monitor mode is off. In case you switch it on, the Remote Console window will be started in a read only mode.

Start in Exclusive Access Mode

Enables the exclusive access mode immediately at Remote Console startup. This forces the Remote Consoles of all other users to close. No one can open the Remote Console at the same time again until this user disables the exclusive access or logs off.

Mouse hotkey

Allows to specify a hotkey combination which starts either the mouse synchronization process if pressed in the Remote Console, or is used to leave the single mouse mode.

Remote Console Button Keys

Button Keys allow simulating keystrokes on the remote system that cannot be generated locally. The reason for this might be a missing key or the fact, that the local operating system of the Remote Console is unconditionally catching this keystroke already. Typical examples are " Control+Alt+Delete " on Windows and DOS, what is always caught, or "Control+Backspace" on Linux for terminating the X-Server. The syntax to define a new Button Key is as follows:

[confirm] <keycode>[+|-[*]<keycode>]*

"confirm" requests confirmation by a dialog box before the key strokes will be sent to the remote host.

"keycode" is the key to be sent. Multiple key codes can be concatenated with a plus, or a minus sign. The plus sign builds key combinations, all keys will be pressed until a minus

sign or the end of the combination is encountered. In this case all pressed keys will be released in reversed sequence. So the minus sign builds single, separate key presses and -releases. The star inserts a pause with duration of 100 milliseconds.

6.4.2 Keyboard/Mouse

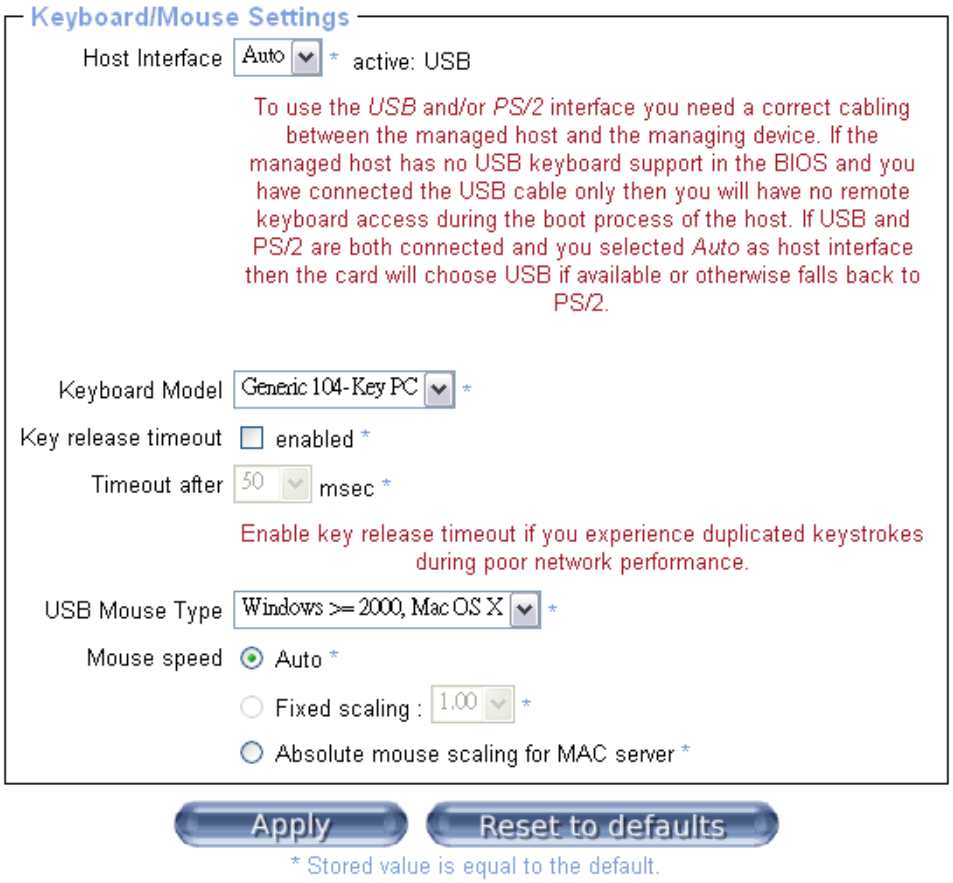

Keyboard/Mouse Settings
Host Interface
Auto
active: USB
To use the USB and/or PS/2 interface you need a correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only then you will have no remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you selected Auto as host interface then the card will choose USB if available or otherwise falls back to PS/2.
Keyboard Model
Generic 104-Key PC
Key release timeout
enabled
Timeout after
50
msec
Enable key release timeout if you experience duplicated keystrokes during poor network performance.
USB Mouse Type
Windows >= 2000, Mac OS X
Mouse speed
Auto
Fixed scaling :
1.00
Absolute mouse scaling for MAC server
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 6-13. Keyboard and Mouse Settings

Host Interface

Enables a certain interface the mouse is connected to. You can choose between "Auto" for automatic detection, "USB" for an USB mouse, and "PS/2" for a PS/2 mouse.

Warning

To use the USB and/or PS/2 interface you need a correct cabling between the managed host and the managing device. If the managed host has no USB keyboard support in the BIOS and you have connected the USB cable only then you will have no remote keyboard access during the boot process of the host. If USB and PS/2 are both connected and you selected " Auto " as host interface, then the card will select " USB " if available or otherwise falls back to " PS/2 ".

To get USB remote keyboard access during the boot process of the host, the following conditions must be fulfilled:

- the host bios must have USB keyboard support
- the USB cable must be connected or must be selected in the Host interface option

PS/2 Keyboard Model

Enables a certain keyboard layout. You can choose between "Generic 101-Key PC" for a standard keyboard layout, "Generic 104-Key PC" for a standard keyboard layout extendend by three additional windows keys, "Generic 106-Key PC" for a japanese keyboard, and "Apple Macintosh" for the Apple Macintosh.

Keyboard timeout
Recommanded as “enable” for keyboard timeout when host is UNIX or UNIX-like OS.

USB Mouse Type

Enables USB mouse type. Choose between "MS Windows 2000 or newer" for MS Windows 2000 or Windows XP, or " Other Operating Systems " for MS Windows NT, Linux, or OS X. In "MS Windows 2000 or newer" mode the remote mouse is always synchronized with the local mouse.

Mouse Speed

- Auto mouse speed

  Use this option if the mouse settings on host use an additional acceleration setting. The BI080135/BI160135 tries to detect the acceleration and speed of the mouse during the mouse sync process.

- Fixed mouse speed

Use a direct translation of mouse movements between the local and the remote pointer.

You may also set a fixed scaling which determines the pixel-amount of the remote mouse pointer movement when the local mouse pointer is moved by one pixel. This option is used to manually control the remote mouse speed and only works when the mouse settings on the host are linear. This means mouse acceleration of OS should be disabled, and the intelligent mouse synchronization of IP-KVM is not functioning under this setting.

- Absolute mouse scaling for MAC server

  Use this option for MAC server.

To set the options, click on the button "Apply".

6.4.3 Video

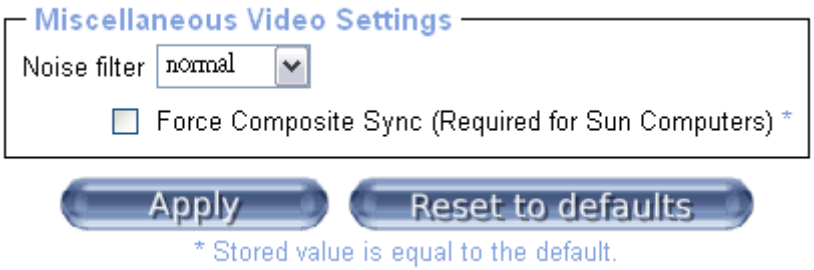


Figure 6-14. Video Settings

Miscellaneous Video Settings

- Noise filter

  This option defines how the BI080135/BI160135 reacts to small changes in the video input signal. A large filter setting needs less network traffic and leads to a faster video display, but small changes in some display regions may not be recognized immediately. A small filter displays all changes instantly but may lead to a constant amount of network traffic even if the display content is not really changing (depending on the quality of the video input signal). All in all the default setting should be suitable for most situations.

- Force Composite Sync (Required for Sun Computers)

  To support signal transmission from a Sun machine, enable this option. If not enabled the picture of the remote console will not be visible.

To set the options, click on the button "Apply".

6.5 Device Settings

6.5.1 Network

The Network Settings panel as shown in Figure 6-19 allows changing network related parameters. Each parameter will be explained below. Once applied the new network settings will immediately come into effect.

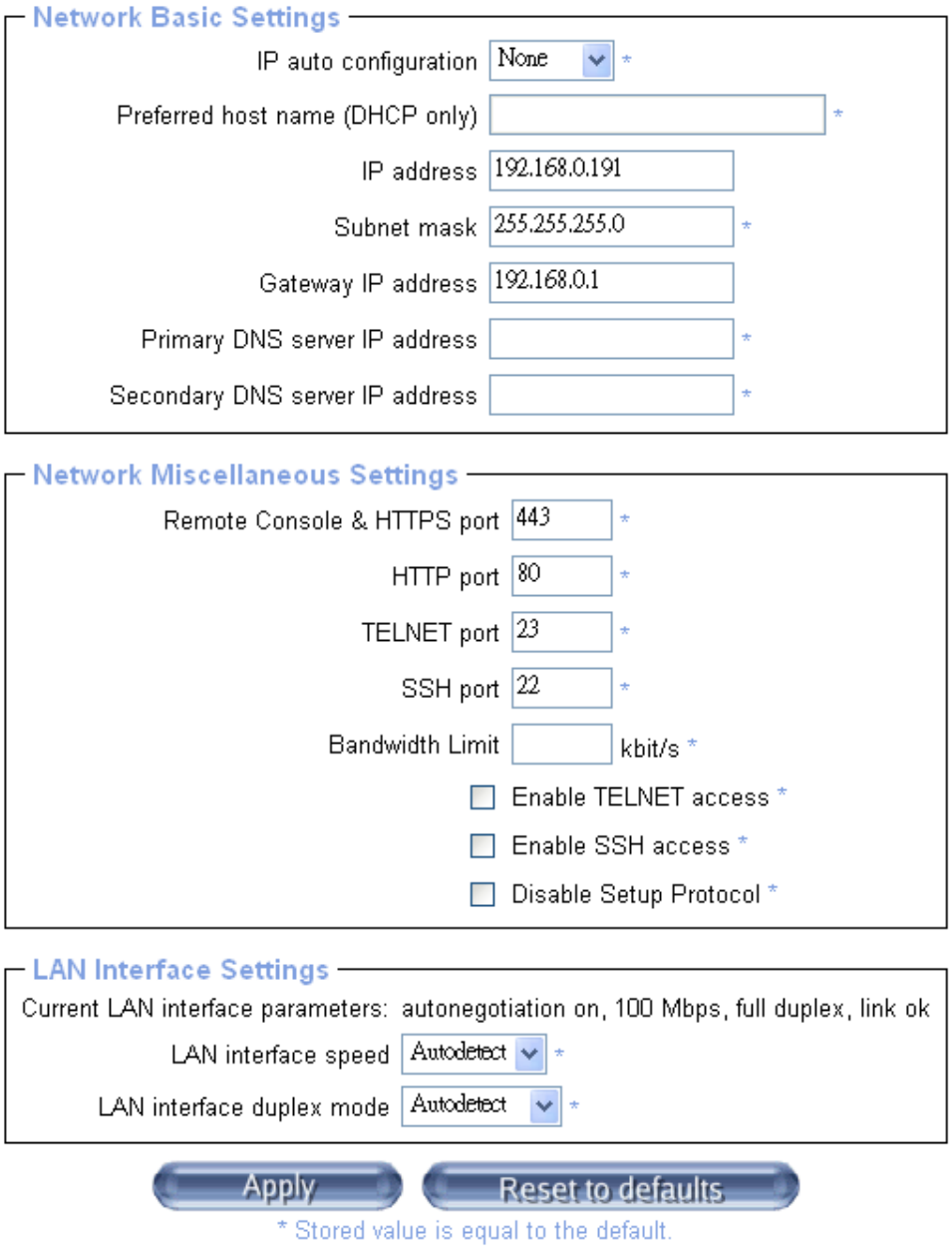


Figure 6-15. Network Settings

Warning

Changing the network settings of the BI080135/BI160135 might result in losing connection to it. In case you change the settings remotely make sure that all the values are correct and you still have an option to access the BI080135/BI160135.

IP auto configuration

With this option you can control if the BI080135/BI160135 should fetch its network settings from a DHCP or BOOTP server. For DHCP, select "dhcp" , and for BOOTP select "bootp" accordingly. If you choose"none" then IP auto configuration is disabled.

IP address

IP address in the usual dot notation.

Subnet Mask

The net mask of the local network.

Gateway IP address

In case the BI080135/BI160135 should be accessible from networks other than the local one, this IP address must be set to the local network router's IP address.

Primary DNS Server IP Address

IP address of the primary Domain Name Server in dot notation. This option may be left empty, however the BI080135/BI160135 will not be able to perform name resolution.

Secondary DNS Server IP Address

IP address of the secondary Domain Name Server in dot notation. It will be used in case the Primary DNS Server cannot be contacted.

Remote Console And HTTPS port

Port number at which the BI080135/BI160135 Remote Console server and HTTPS server are listening. If left empty the default value will be used.

HTTP port

Port number at which the BI080135/BI160135 HTTP server is listening. If left empty the default value will be used.

Telnet port

Port number at which the BI080135/BI160135 Telnet server is listening. If left empty the default value will be used.

Bandwidth limitation

The maximum network traffic generated through the BI080135/BI160135 ethernet device. Value in Kbit/s.

Enable Telnet access

Set this option to allow accessing the LARA express using the Telnet
Gateway see the Section called Telnet Console).

Disable Setup Protocol

Enable this option to exclude the BI080135/BI160135 from the setup protocol.

6.5.2 Dynamic DNS

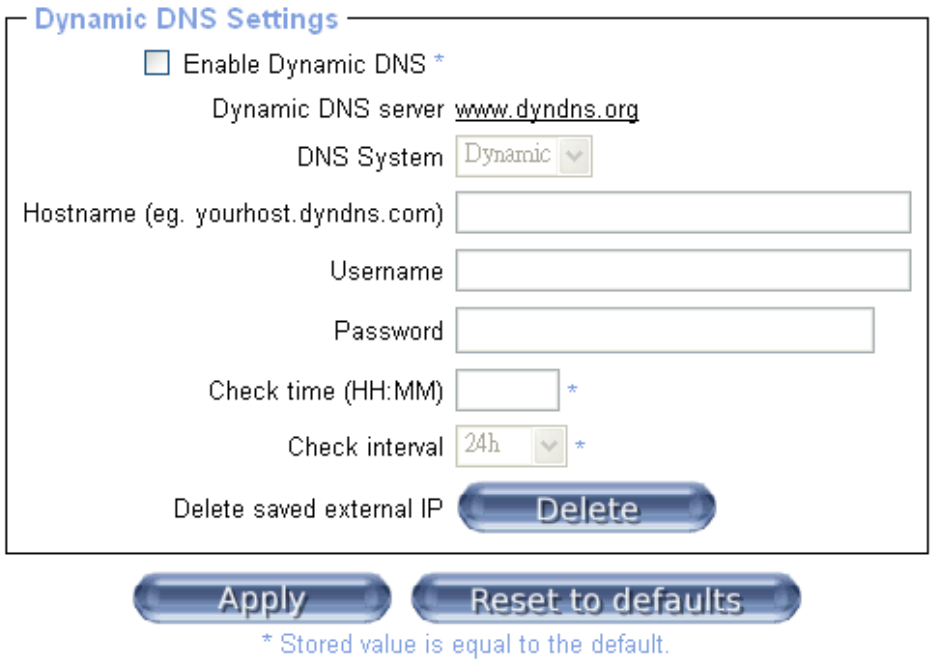


Figure 6-16. Dynamic DNS

A freely available Dynamic DNS service (dyndns.org) can be used in the following scenario (see Figure 6-21):

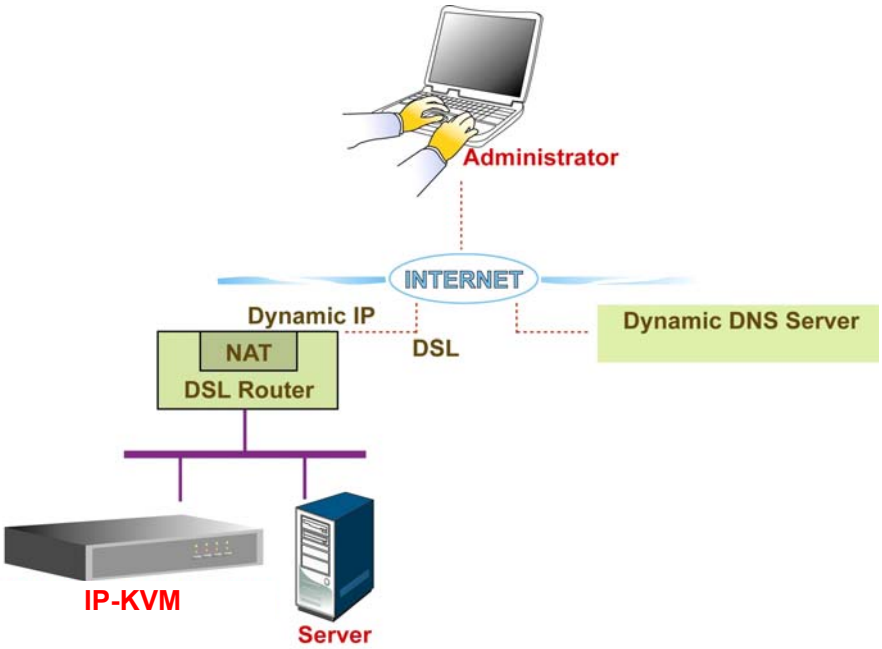


Figure 6-17. Dynamic DNS Scenario

The BI080135/BI160135 is reachable via the IP address of the DSL router, which is dynamically assigned by the provider. Since the administrator does not know the IP address assigned by the provider, the BI080135/BI160135 connects to a special dynamic DNS server in regular

intervals and registers its IP address there. The administrator may contact this server as well and pick up the same IP address belonging to his card.

The administrator has to register a BI080135/BI160135 that is supposed to take part in the service with the Dynamic DNS Server and assign a certain hostname to it. He will get a nickname and a password in return to the registration process. This account information together with the hostname is needed in order to determine the IP address of the registered BI080135/BI160135.

You have to perform the following steps in order to enable Dynamic DNS:

- Make sure that the LAN interface of the BI080135/BI160135 is properly configured.
- Enter the Dynamic DNS Settings configuration dialog as shown in Figure 6-20.
- Enable Dynamic DNS and change the settings according to your needs (see below).

Enable Dynamic DNS

This enables the Dynamic DNS service. This requires a configured DNS server IP address.

Dynamic DNS server

This is the server name where BI080135/BI160135 registers itself in regular intervals. Currently, this is a fixed setting since only dyndns.org is supported for now.

Hostname

This is the hostname of the BI080135/BI160135 that is provided by the Dynamic DNS Server. (Use the whole name including the domain, e.g. testserver.dyndns.org, not just the actual hostname).

Username

You have registered this username during your manual registration with the Dynamic DNS Server. Spaces are not allowed in the Nickname.

Password

You have used this password during your manual registration with the Dynamic DNS Server.

Check time

The BI080135/BI160135 card registers itself in the Dynamic DNS server at this time.

Check interval

This is the interval for reporting again to the Dynamic DNS server by the BI080135/BI160135.

Warning

The BI080135/BI160135 has its own independent real time clock. Make sure the time setting of the BI080135/BI160135 is correct. (See the Section called *Date And Time)*

6.5.3 Security

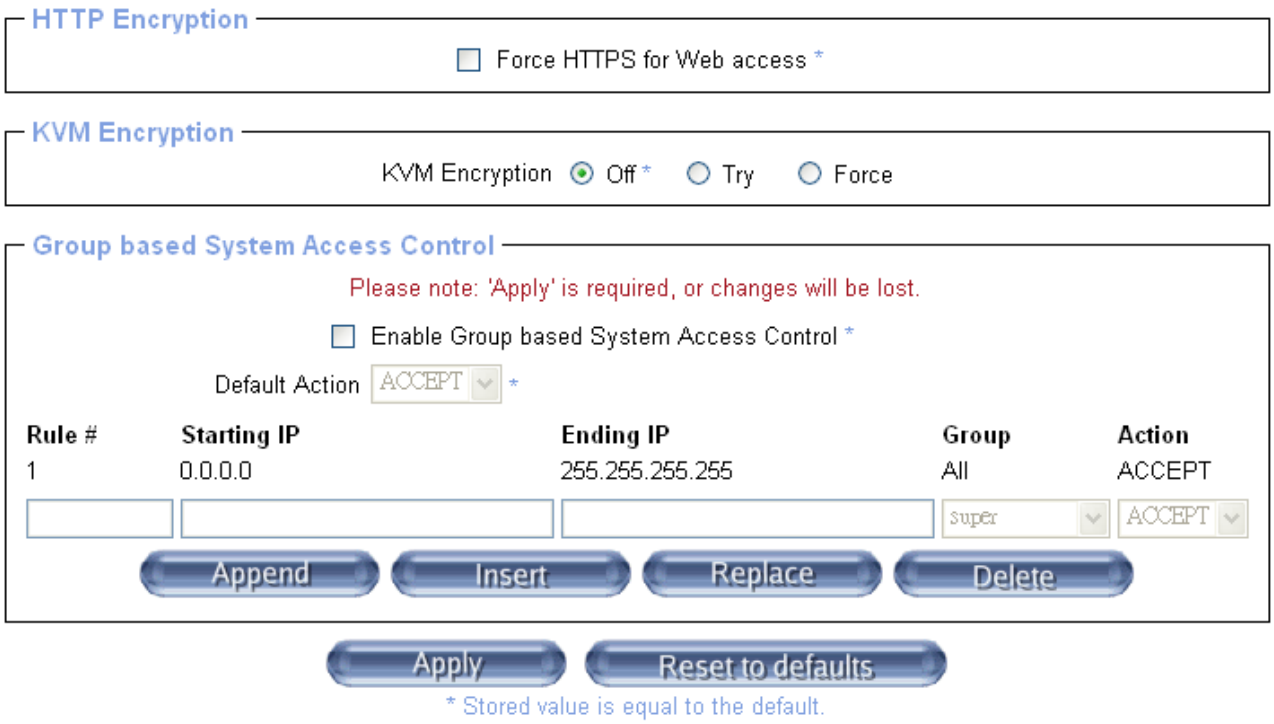

HTTP Encryption
Force HTTPS for Web access *
KVM Encryption
KVM Encryption Off * Try Force
Group based System Access Control
Please note: 'Apply' is required, or changes will be lost.
Enable Group based System Access Control *
Default Action ACCEPT *
Rule # Starting IP Ending IP Group Action
1 0.0.0.0 255.255.255.255 All ACCEPT
super ACCEPT
Append Insert Replace Delete
Apply Reset to defaults
* Stored value is equal to the default.

Figure 6-18. Device Security

Force HTTPS

If this option is enabled access to the web front-end is only possible using an HTTPS connection. The BI080135/BI160135 will not listen on the **HTTP** port for incoming connections.

In case you want to create your own SSL certificate that is used to identify the BI080135/BI160135 refer to the Section called *Certificate.*

KVM encryption

This option controls the encryption of the RFB protocol. RFB is used by the Remote Console to transmit both the screen data to the administrator machine and keyboard and mouse data back to the host. If set to 'Off' no encryption will be used. If set to Try' the applet tries to make an encrypted connection. In case connection establishment fails for any reason an unencrypted connection will be used.

If set to "Force" the applet tries to make an encrypted connection. An error will be reported in case connection establishment fails.

Group-based System Access Control

This is the IP filtering function, it keeps unauthorized hosts from accessing to the IP-KVM by specifying IP filtering rules. It is important to fully understand what an IP filter is. If you don't fully understand this, you will get unexpected results against your original plan.

Chain rule

The **Chain rule** determines whether the access from the hosts is allowed or not. It can be one of these two values:

- ACCEPT : access allowed
- DROP : access not allowed

The rule can be configured to apply to a particular Group level (All, User, Super, Administrator).

When the IP-KVM receives a TCP packet, it will process the packet with the chain rule depicted below. The process ordering is important; The packet will enter the chain rule 1 first, if meet the rule then take action directly, otherwise go to chain rule 2.

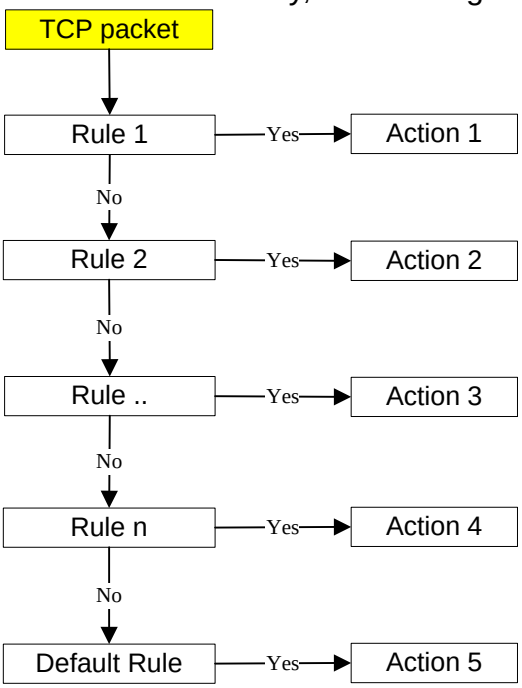
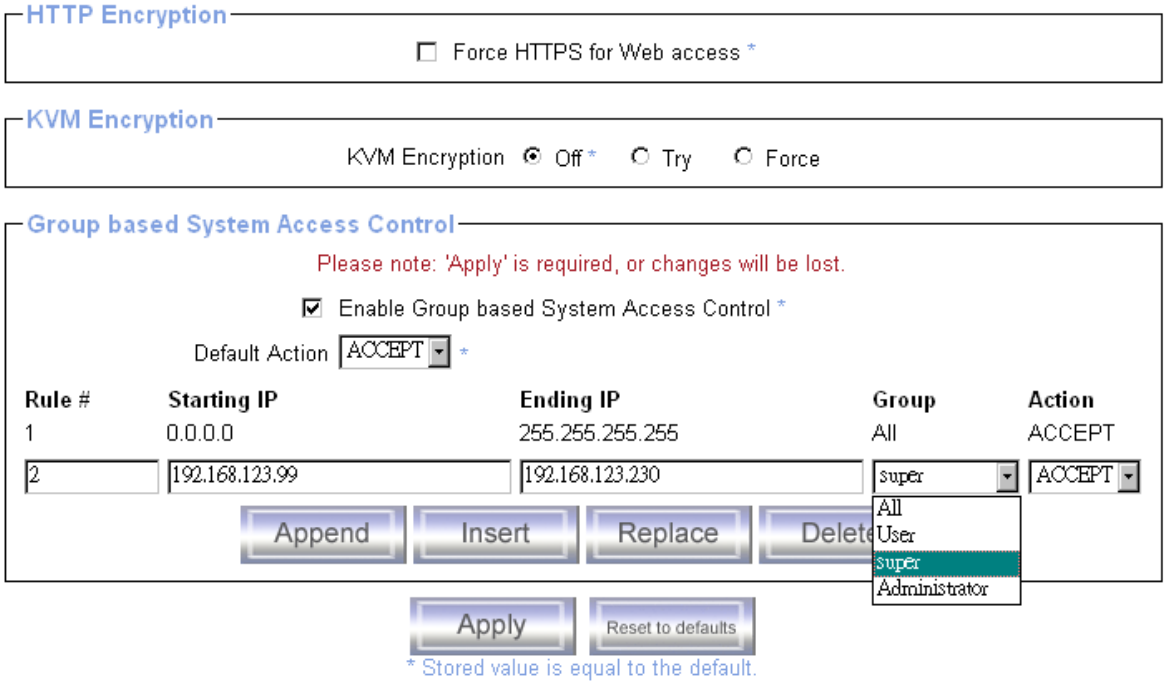


Figure 6-19 Chain Rules of IP Filtering

Check the “Enable Group based System Access Control” to edit the rules

Users can add a new IP filtering rule by setting the properties at adding line by **Append** or **Insert**. User can remove a rule by **Remove** or **Delete**.



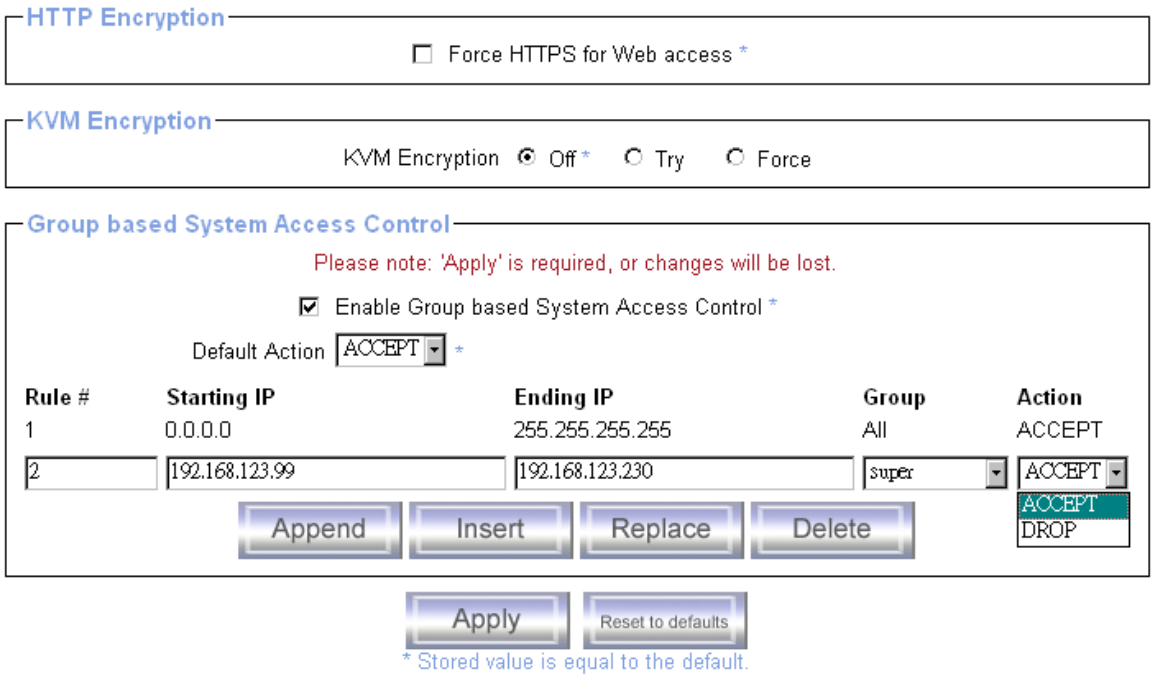

HTTP Encryption
Force HTTPS for Web access *
KVM Encryption
KVM Encryption Off * Try Force
Group based System Access Control
Please note: 'Apply' is required, or changes will be lost.
Enable Group based System Access Control *
Default Action ACCEPT *
Rule # Starting IP Ending IP Group Action
1 0.0.0.0 255.255.255.255 All ACCEPT
2 192.168.123.99 192.168.123.230 super ACCEPT
ACCEPT
DROP
Append Insert Replace Delete
Apply Reset to defaults
* Stored value is equal to the default.

Figure 6-20

6.5.4 Certificate

Figure 6-21. Certificate Settings

The BI080135/BI160135 uses the Secure Socket Layer (SSL) protocol for any encrypted network traffic between itself and a connected client. During the connection establishment the BI080135/BI160135 has to expose its identity to a client using a cryptographic certificate. Upon delivery, this certificate and the underlying secret key is the same for all BI080135/BI160135 ever produced and certainly will not match the network configuration that will be applied to the BI080135/BI160135 cards by its user. The certificate's underlying secret key is also used for securing the SSL handshake. Hence, this is a security risk (but far better than no encryption at all).

However, it is possible to generate and install a new certificate that is unique for a particular BI080135/BI160135 card. In order to do that, the BI080135/BI160135 is able to generate a new cryptographic key and the associated Certificate Signing Request (CSR) that needs to be certified by a certification authority (CA). A certification authority verifies that you are the person who you claim you are, and signs and issues a SSL certificate to you.

The following steps are necessary to create and install a SSL certificate for the BI080135/BI160135:

• Create a SSL Certificate Signing Request using the panel shown in Figure 6-23. You need to fill out a number of fields that are explained below. Once this is done, click on the button " Create " which will initiate the Certificate Signing Request generation. The CSR can be downloaded to your administration machine with the "Download CSR" button (see Figure 6-24).

• Send the saved CSR to a CA for certification. You will get the new certificate from the CA after a more or less complicated traditional authentication process (depending on the CA).

• Upload the certificate to the BI080135/BI160135 using the "Upload" button as shown in Figure 6-24.

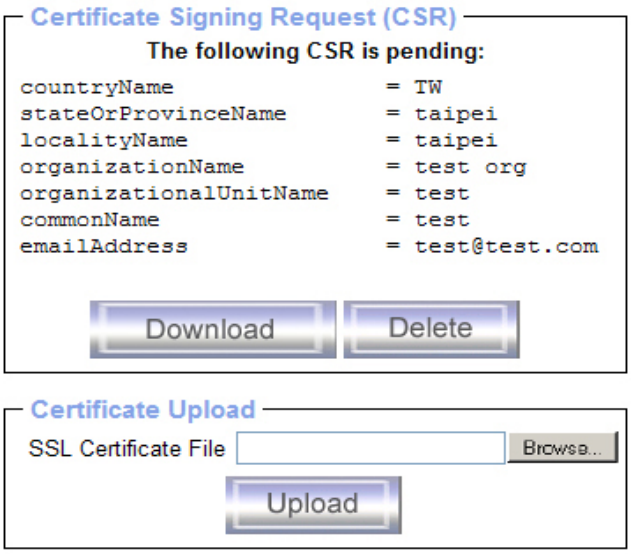


Figure 6-22. SSL Certificate Upload

After completing these three steps, the BI080135/BI160135 has its own certificate that is used for identifying the card to its clients.

Warning

If you destroy the CSR on the BI080135/BI160135 there is no way to get it back! In case you deleted it by mistake, you have to repeat the three steps as described above.

Common name

This is the network name of the BI080135/BI160135 once it is installed in the user's network (usually the fully qualified domain name). It is identical to the name that is used to access the BI080135/BI160135 with a web browser (without the "http://" prefix). In case the name given here and the actual network name differ, the browser will pop up a security warning when the BI080135/BI160135 is accessed using HTTPS.

Organizational unit

This field is used for specifying to which department within an organization the BI080135/BI160135 belongs.

Organization

The name of the organization to which the BI080135/BI160135 belongs.

Locality/City

The city where the organization is located.

State/Province

The state or province where the organization is located.

Country (ISO code)

The country where the organization is located. This is the two-letter ISO code, e.g. DE for Germany, or US for the USA.

Challenge Password

Some certification authorities require a challenge password to authorize later changes on the certificate (e.g. revocation of the certificate). The minimal length of this password is 4 characters.

Confirm Challenge Password

Confirmation of the Challenge Password

Email

The email address of a contact person that is responsible for the BI080135/BI160135 and its security.

Key length

This is the length of the generated key in bits. 1024 Bits are supposed to be sufficient for most cases. Longer keys may result in slower response time of the BI080135/BI160135 during connection establishment.

6.5.5 Serial Port

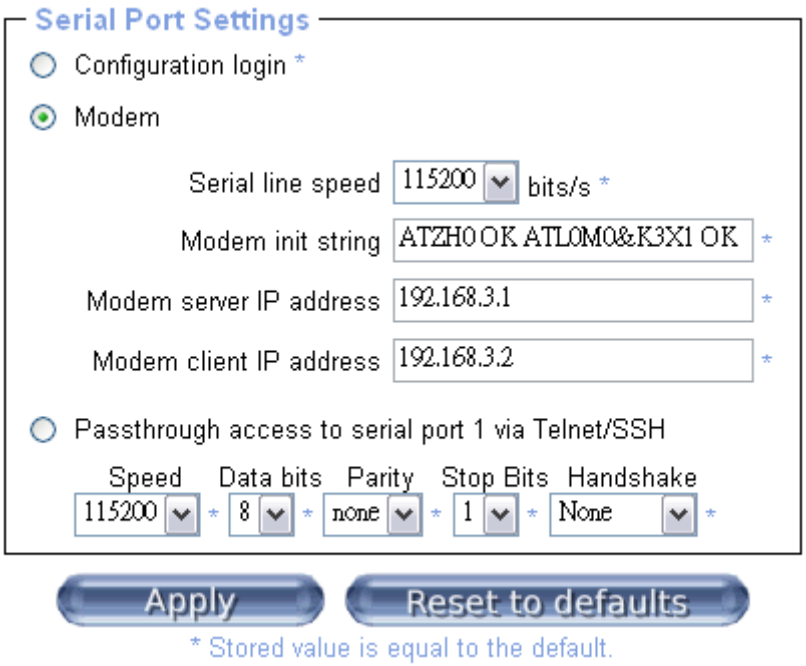

Serial Port Settings
Configuration login *
Modem
Serial line speed 115200 bits/s *
Modem init string ATZH0 OK ATL0M0&K3X1 OK *
Modem server IP address 192.168.3.1 *
Modem client IP address 192.168.3.2 *
Passthrough access to serial port 1 via Telnet/SSH
Speed Data bits Parity Stop Bits Handshake
115200 * 8 * none * 1 * None *
Apply
Reset to defaults
* Stored value is equal to the default.

Figure 6-23. Serial Port

The BI080135/BI160135 Serial Settings (Figure 6-25) allow you to specify what device is connected to the serial port and how to use it.

Configuration or console login

Do not use the serial port for any special function, use it only for the initial configuration (see Table 4-1).

Modem

The BI080135/BI160135 offers remote access using a telephone line in addition to the standard access over the built-in Ethernet adapter. The modem needs to be connected to the serial interface of the BI080135/BI160135 .

Logically, connecting to the BI080135/BI160135 using a telephone line means nothing else than building up a dedicated point-to-point connection from your console computer to the BI080135/BI160135. In other words, the BI080135/BI160135 acts as an Internet Service Provider (ISP) to which you can dial in. The connection is established using the Point-to-Point Protocol (PPP). Before you connect to the BI080135/BI160135, make sure to configure your console computer accordingly. For instance, on Windows based operating systems you can configure a dial-up network connection, which defaults to the right settings like PPP.

The Modem Settings panel allows you to configure the remote access to the BI080135/BI160135 using a modem. The meaning of each parameter will be described below. The modem settings are part of the serial settings panel.

Serial line speed

The speed the BI080135/BI160135 is communicating with the modem. Most of all modems available today will support the default value of 115200 bps. In case you are using an old modem and discovering problems try to lower this speed.

Modem Init String

The initialization string used by the BI080135/BI160135 to initialize the modem. The default value will work with all modern standard modems directly connected to a telephone line. In case you have a special modem or the modem is connected to a local telephone switch that requires a special dial sequence in order to establish a connection to the public telephone network, you can change this setting by giving a new string. Refer to the modem's manual about the AT command syntax.

Modem server IP address

This IP address will be assigned to the BI080135/BI160135 itself during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure, it is not interfering with the IP settings of the BI080135/BI160135 and your console computer. The default value will work in most cases.

Modem client IP address

This IP address will be assigned to your console computer during the PPP handshake. Since it is a point-to-point IP connection virtually every IP address is possible but you must make sure, it is not interfering with the IP settings of the BI080135/BI160135 and your console computer. The default value will work in most cases.

Passthrough access to serial port via Telnet

Using this option, it is possible to connect an arbitrary device to the serial port and access it (assuming it provides terminal support) via Telnet. Select the appropriate options for the serial port and use the Telnet Console, or a standard Telnet client to connect to the BI080135/BI160135 .

6.5.6 Date And Time

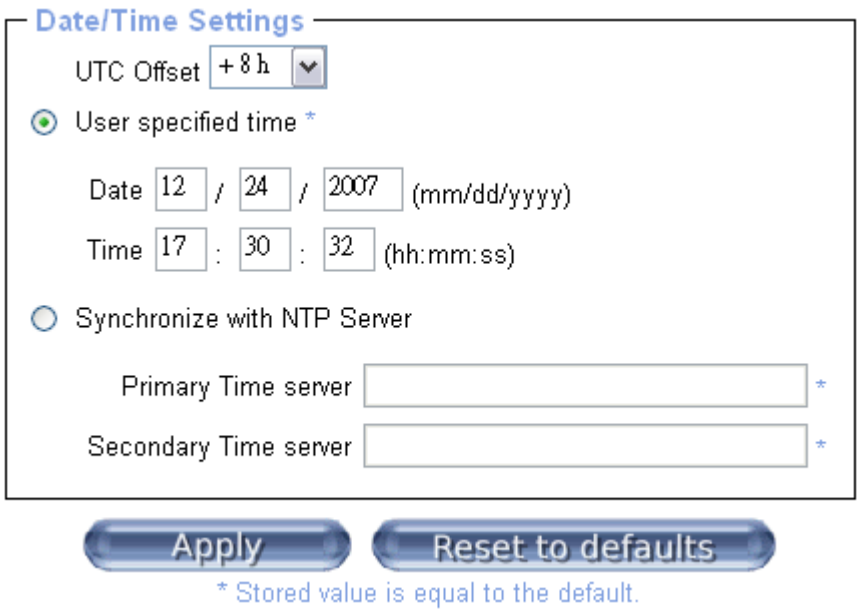


Figure 6-24. Date and Time

This link refers to a page, where the internal real-time clock of the BI080135/BI160135 can be set up (see Figure 6-27). You have the possibility to adjust the clock manually, or to use a NTP timeserver. Without a timeserver, your time setting will not be persistent, so you have to adjust it again, after BI080135/BI160135 loses power for more than a few minutes. To avoid this, you can use a NTP timeserver, which sets up the internal clock automatically to the current UTC time. Because NTP server time is always UTC, there is a setting that allows you to set up a static offset to get your local time.

Warning

There is currently no way to adjust the daylight saving time automatically. So you have to set up the UTC offset twice a year properly to the local rules of your country.

6.5.7 Event Log

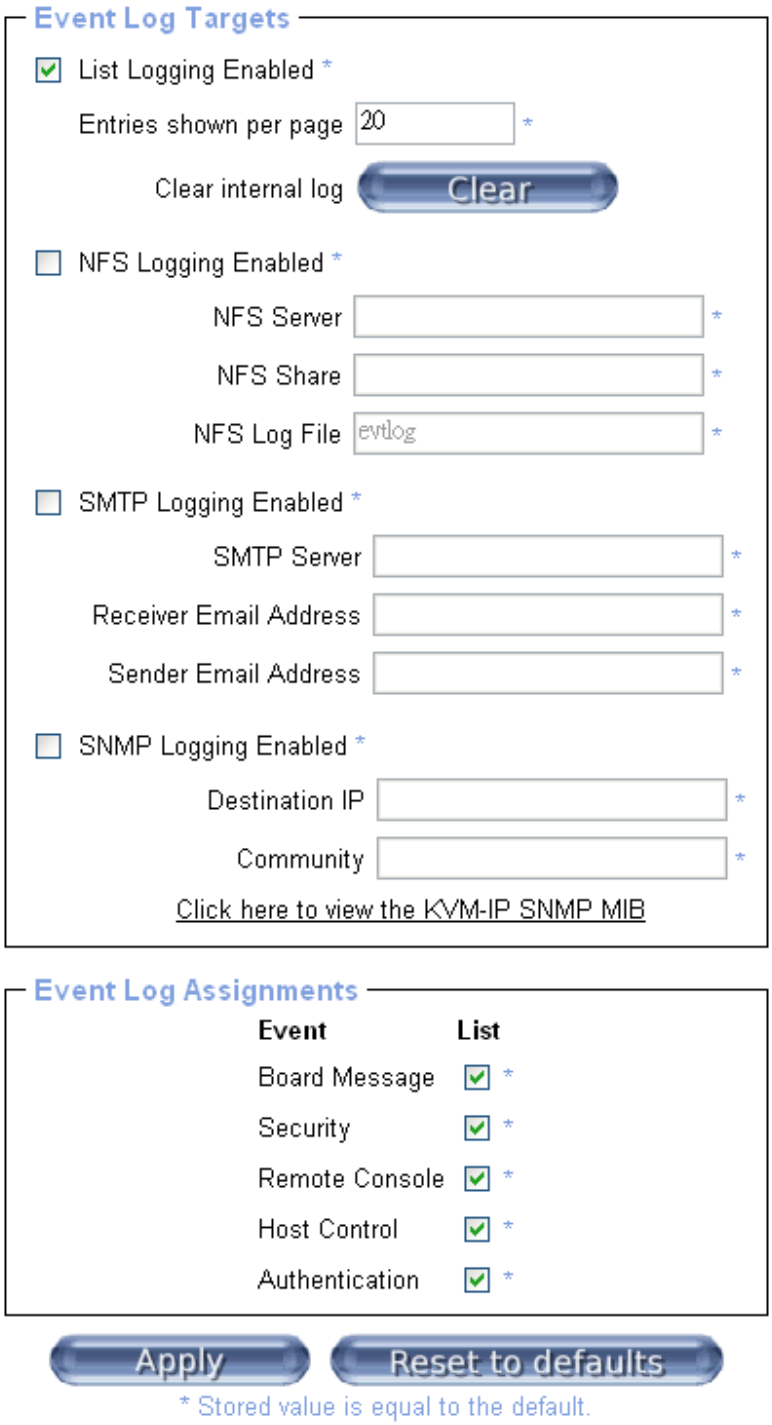


Figure 6-25. Event Log

Important events like a login failure or a firmware update are logged to a selection of logging destinations (see Figure 6-29). Each of those events belongs to an event group, which can be activated separately.

The common way to log events is to use the internal log list of the BI080135/BI160135. To show the log list, click on "Event Log" on the "Maintenance" page. In the Event Log Settings you can choose how many log entries are shown on each page. Furthermore, you can clear the log file here.

List logging enabled

The common way to log events is to use the internal log list of the BI080135/BI160135 . To

show the log list, click on "Event Log" on the "Maintenance" page.

Since the BI080135/BI160135 system memory is used to save all the information, the maximum number of possible log list entries is restricted to 1.000 events. Every entry that exceeds this limit overrides the oldest one, automatically.

Warning

If the reset button on the HTML front-end is used to restart the BI080135/BI160135, all logging information is saved permanently and is available after the BI080135/BI160135 has been started. If the BI080135/BI160135 loses power or a hard reset is performed, all logging data will be lost. To avoid this, use one of the following log methods.

NFS Logging enabled

Define a NFS server, where a directory or a static link have to be exported, to write all logging data to a file that is located there. To write logging data from more than one BI080135/BI160135 devices to only one NFS share, you have to define a file name that is unique for each device. When you change the NFS settings and press the button "Apply" ,the NFS share will be mounted immediately. That means, the NFS share and the NFS server must be filled with valid sources or you will get an error message.

SMTP Logging enabled

With this option, the BI080135/BI160135 is able to send Emails to an address given by the Email address text field in the Event Log Settings. These mails contain the same description strings as the internal log file and the mail subject is filled with the event group of the occurred log event. In order to use this log destination you have to specify a SMTP server, that has to be reachable from the BI080135/BI160135 device and that needs no authentication at all (<serverip>:<port>).

SNMP Logging enabled

If this is activated, the BI080135/BI160135 sends a SNMP trap to a specified destination IP address, every time a log event occurs. If the receiver requires a community string, you can set it in the appropriate text field. Most of the event traps only contain one descriptive string with all information about the log event. Only authentication and host power events have an own trap class that consists of several fields with detailed information about the occurred event. To receive this SNMP traps, any SNMP trap listener may be used.

Warning

In contrast to the internal log file on the BI080135/BI160135, the size of the NFS log file is not limited. Every log event will be appended to the end of the file so it grows continuously and you may have to delete it or move it away from time to time.

6.6 Maintenance

6.6.1 Device Information

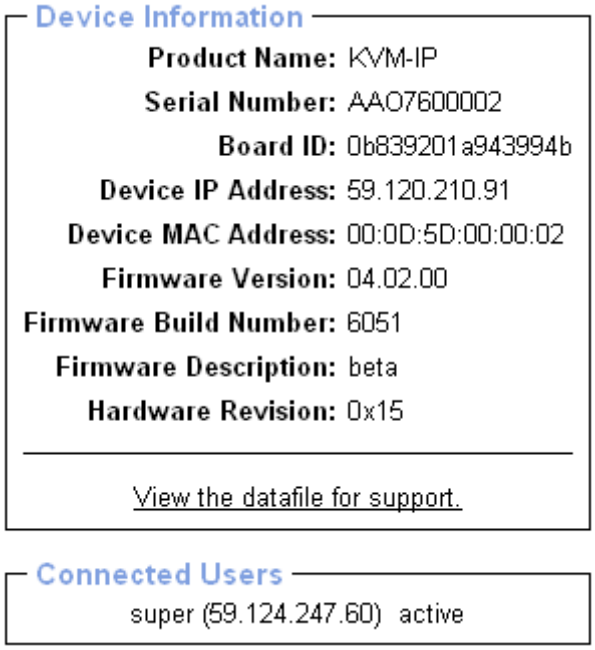


Figure 6-26. Device Information

Board Summary

This section contains a summary with various information about this **IP-KVM** and it's current firmware and allows you to reset the card. You may have a look at Figure 6-29 for an example.

The Data file for support allows you to download the **IP-KVM** data file with specific support information. This is an XML file with certain customized support information like the serial number etc. You may send us this information together with a support request. It will help us to locate and solve your reported problem.

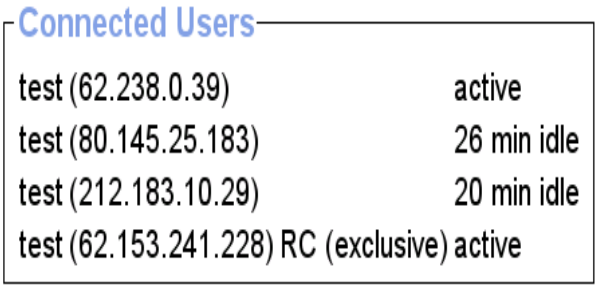

Connected Users
test (62.238.0.39) active
test (80.145.25.183) 26 min idle
test (212.183.10.29) 20 min idle
test (62.153.241.228) RC (exclusive) active

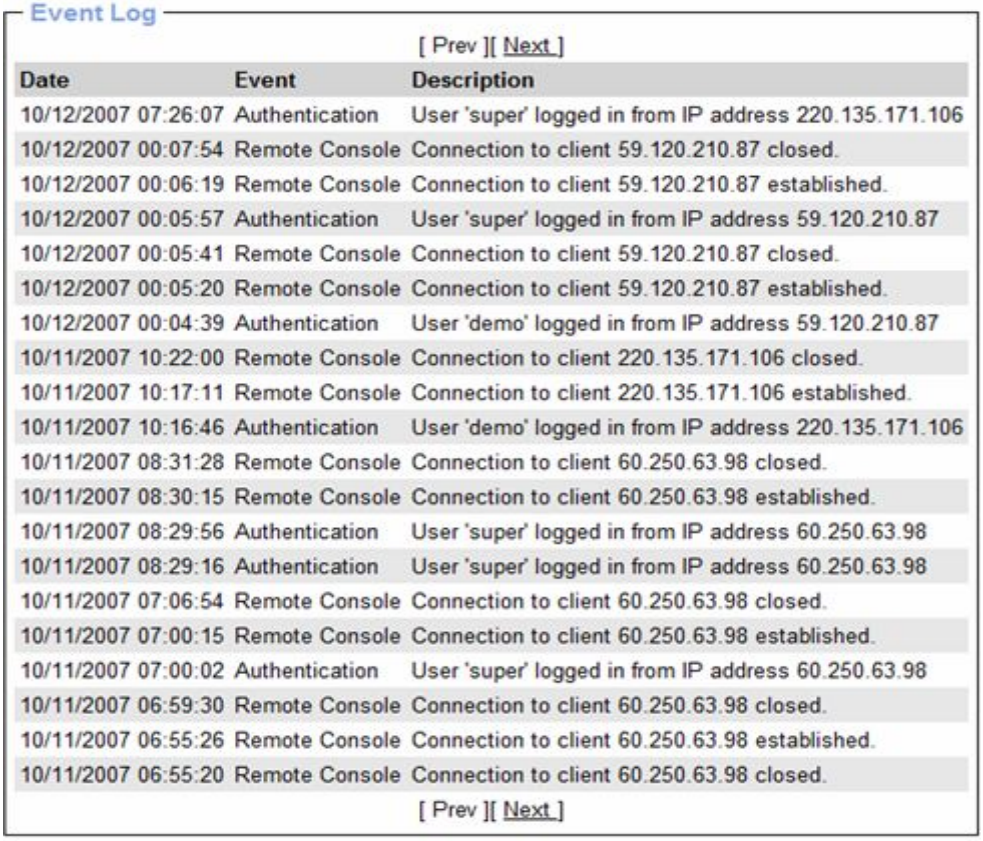
Figure 6-27. Connected Users

Figure 6-27 displays the IP-KVM activity. From left to right the connected user(s), its IP address (from which host the user comes from) and its activity status is displayed. RC means that the Remote Console is open. If the Remote Console is opened in exclusive mode the term (exclusive mode) is added. For more information about this option see the Section called Remote Console Control Bar in Chapter 5. To display the user activity the last column contains either the term active for an active user or 20 min idle for a user who is inactive for a certain amount of time.

Reset Functions

This section allows you to reset specific parts of the device. Currently this involves the video engine and the BI080135/BI160135 itself. Resetting the card itself is mainly needed to activate a newly updated firmware. It will close all current connections to the administration console and to the Remote Console. The whole process will take about half a minute. Resetting sub devices (e.g. video engine) will take some seconds only and do not result in closing connections.

6.6.2 Event Log


Event Log

[Prev][Next]

Date	Event	Description
10/12/2007 07:26:07	Authentication	User 'super' logged in from IP address 220.135.171.106
10/12/2007 00:07:54	Remote Console	Connection to client 59.120.210.87 closed.
10/12/2007 00:06:19	Remote Console	Connection to client 59.120.210.87 established.
10/12/2007 00:05:57	Authentication	User 'super' logged in from IP address 59.120.210.87
10/12/2007 00:05:41	Remote Console	Connection to client 59.120.210.87 closed.
10/12/2007 00:05:20	Remote Console	Connection to client 59.120.210.87 established.
10/12/2007 00:04:39	Authentication	User 'demo' logged in from IP address 59.120.210.87
10/11/2007 10:22:00	Remote Console	Connection to client 220.135.171.106 closed.
10/11/2007 10:17:11	Remote Console	Connection to client 220.135.171.106 established.
10/11/2007 10:16:46	Authentication	User 'demo' logged in from IP address 220.135.171.106
10/11/2007 08:31:28	Remote Console	Connection to client 60.250.63.98 closed.
10/11/2007 08:30:15	Remote Console	Connection to client 60.250.63.98 established.
10/11/2007 08:29:56	Authentication	User 'super' logged in from IP address 60.250.63.98
10/11/2007 08:29:16	Authentication	User 'super' logged in from IP address 60.250.63.98
10/11/2007 07:06:54	Remote Console	Connection to client 60.250.63.98 closed.
10/11/2007 07:00:15	Remote Console	Connection to client 60.250.63.98 established.
10/11/2007 07:00:02	Authentication	User 'super' logged in from IP address 60.250.63.98
10/11/2007 06:59:30	Remote Console	Connection to client 60.250.63.98 closed.
10/11/2007 06:55:26	Remote Console	Connection to client 60.250.63.98 established.
10/11/2007 06:55:20	Remote Console	Connection to client 60.250.63.98 closed.

[Prev][Next]

Figure 6-28. Event Log List

Figure 6-28 displays the log list including the events that are logged by the BI080135/BI160135.

6.6.3 Update Firmware

The BI080135/BI160135 is a complete standalone computer. The software it runs is called firmware. The firmware of the BI080135/BI160135 can be updated remotely in order to install new functionality or special features.

A new firmware update is a binary file which will be sent to you by email or which you can download from the supplier web site. If the firmware file is compressed (file suffix .zip) then you must unzip it before you can proceed. Under the Windows operating system you may use WinZip from http://www.winzip.com/ for decompression. Other operating systems might provide a program called unzip.

Before you can start updating the firmware of your BI080135/BI160135 the new uncompressed firmware file has to be accessible on the system that you use for connecting to the BI080135/BI160135.

Updating the firmware is a three-stage process:

- Firstly, the new firmware file is uploaded onto the BI080135/BI160135. In order to do that you need to select the file on your local system using the button “Browse” of the Upload Firmware panel. Once the firmware file has been uploaded, it is checked whether it is a valid firmware file and whether there were any transmission errors. In case of any error the Upload Firmware function will be aborted.

• Secondly, if everything went well, you see the Update Firmware panel. The panel shows you the version number of the currently running firmware and the version number of the uploaded firmware. Pressing the button “Update” will store the new version and substitute the old one completely.

Warning

This process is not reversible and might take some minutes. Make sure the BI080135/BI160135 power supply will not be interrupted during the update process, because this may cause an unusable card.

• Thirdly, after the firmware has been stored, the panel will request you to reset the BI080135/BI160135 manually. Half a minute after the reset, the BI080135/BI160135 will run with the new firmware version and should be accessible. However, you are requested to login once again.

Warning

The three-stage firmware update process and complete consistency check are making a mistake in updating the firmware almost impossible. However, only experienced staff members or administrators should perform a firmware update. Make sure the BI080135/BI160135 power supply will not be interrupted!

6.6.4 Unit Reset

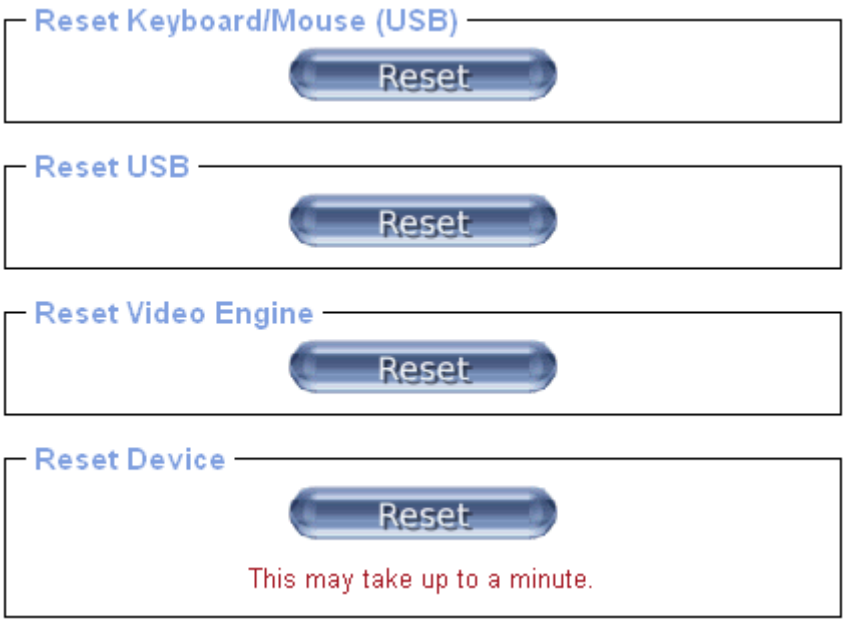


Figure 6-30. Unit Reset

This section allows you to reset specific parts of the device. This involves the both keyboard and mouse, the video engine and the BI080135/BI160135 itself. Resetting the card itself is mainly needed to activate a newly updated firmware. It will close all current connections to the administration console and to the Remote Console.

The whole process will take about half a minute. Resetting sub devices (e.g. video engine) will take some seconds only and does not result in closing connections. To reset a certain

BI080135/BI160135 functionality click on the button Reset as displayed in Figure 6-34.

Note: Only the super user is allowed to reset the BI080135/BI160135.

7. Troubleshooting

1. Ensure that all cables are well seated. Label all of cables with the number for each respective computer to avoid confusion.

2. The recommended VGA cable of PC port distance is 5 meters maximum without ghosting and degradation. Normally, the cable length is based on driver capacity of your VGA card. If you need longer VGA cable, please use VGA extender to accomplish your applications.

3. The recommended PS/2 cable of PC port distance is 5 meters maximum. Normally, the cable length is based on driver capacity of your motherboard PS/2 port. If you need longer PS/2 cable, please use PS/2 extender to accomplish your applications.

4. The Power Jack polarity is center positive and the power adapter need be DC5V, 2.6A.

5. Don't press any keys on the keyboard while the selected computer is booting up. Otherwise, it might cause the keyboard error or keyboard is not detected at PC side.

6. The computer boot up fine, but keyboard doesn't work
   Make sure the keyboard works when directly plugged into the computer.
   Try a different keyboard, but use only 101, 102 or 104-key keyboard.

7. The Mouse is not detected during PC boot up.

- Make sure the mouse works when directly plugged into the computer.
- Make sure the mouse is a true PS/2 mouse. A combo mouse will work just as long as it is set for PS/2 mode with the correct adapter. Try a different mouse.
- Avoiding moving the mouse or pressing the mouse buttons when switching ports or during boot up process.
- Avoiding switching ports during shutting down the PC process.
- When you switch one PC port to another PC port, the best scan time setting need to be set to 5 sec. or more. Normally, the VGA monitor change one resolution mode to another will take one or two seconds. So, the scan time is not recommended to below 5 seconds.

8. The power switch is off, but the switch still works fine or power adapter is unplugged from the switch, but the switch still works fine.
   KVM Switch unit draws the power source from power adapter and all PC's PS/2 port. Some PC's PS/2 port can support enough power for the switch, but some PC's PS/2 port (like laptop, notebook computer... etc.) is unable to supply enough power for the switch. In order to make sure the system can work steadily, please do not set power switch to off state or remove the power adapter from the switch.

9. If forgetting the " password " you typed, please contact your supplier.

10. The remote mouse doesn't work or is not synchronous Make sure the mouse settings in BI080135/BI160135 match the mouse model. There are some circumstances where the mouse synchronization process could behave incorrectly, refer to Section 5.4.3 for further explanation.

11. Login on BI080135/BI160135 fails. Was the correct combination of user and password given? On delivery, the user " super " has the password " BI080135/BI160135" depending on the actual device. Moreover your browser must be configured to accept cookies.

12. The Remote Console window can't connect to BI080135/BI160135

    Possibly a firewall prevents access to the Remote Console. Make sure the TCP port numbers 443 or 80 are open for incoming TCP connection establishments.

13. No connection can be established to BI080135/BI160135.

Check whether the network connection is working in general (ping the IP address of BI080135/BI160135). If not, check network hardware. Is BI080135/BI160135 powered on? Check whether the IP address of BI080135/BI160135 and all other IP related settings are correct! Also verify that all the IP infrastructure of your LAN, like routers etc., is correctly configured. Without a ping functioning, BI080135/BI160135 can't work either.

14. In the browser the BI080135/BI160135 pages are inconsistent or chaotic.
    Make sure your browser cache settings are feasible. Especially make sure the cache settings are not set to something like "never check for newer pages". Otherwise BI080135/BI160135 pages may be loaded from your browser cache and not from the card.

15. Using MacOS X a HTTPS connection fails
    You have to install the BI080135/BI160135 certificate using our certificate installer, available on the utility CD. Please refer to the instructions on this CD for further information how to install the certificate.

16. Can't upload the signed certificate in MacOS X
    If an 'internal error' occurs while uploading the signed certificate either change the extension of the file to .txt or add a file helper using the Internet Explorer preferences for this type of file. Make sure that the encoding is plain text and the checkbox 'use for outgoing' is checked. Another possibility is to use a Mozilla based browser.

17. Every time I open a dialog box with some buttons the mouse pointers are not synchronous anymore
    Please check, if you have an option like "'Automatically move mouse pointer to the default button of dialog boxes" enabled in the mouse settings of the operating system. This option needs to be disabled.

18. Remote Console doesn't open with Opera in Linux
    Some versions of Opera don't grant enough permission if the signature of the applet can't be verified. You can add the lines grant code Base "nn.pp.rc.RemoteConsoleApplet" {permission java.lang.RuntimePermission "accessClassInPackage.sun.*";};to the java policy file of opera (e.g. /usr/share/opera/java/opera.policy) to solve the problem.

8. Certificates

FCC

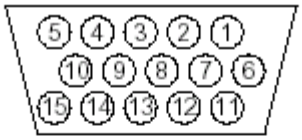
This equipment has been tested and found to comply with Part 15 of the FCC Rules.
Operation is subject to the following two conditions:
(1) This device may not cause harmful interference
(2) This device must accept any interference received. Including interference that may cause undesired operation.

CE - **Certificate**

This equipment is in compliance with the requirements of the following regulations: EN 55 022: CLASS B

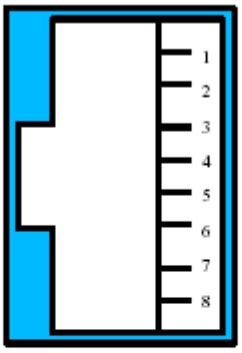
A. Pin Assignments

A.1 VGA HD-15



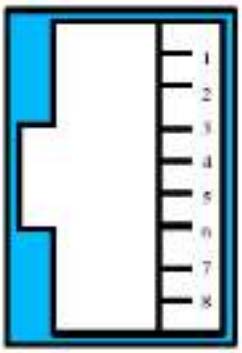
Pin	Assignment	Pin	Assignment
1	Red	9	5 V
2	Green	10	GND sync
3	Blue	11	Not connected
4	Not connected	12	SDA, DDC, ...
5	GND	13	HSYNC
6	GND red	14	VSYNC
7	GND green	15	DATA_CLOCK
8	GND blue		

A.2 RJ 45 Connector Ethernet



Pin	Assignment	Pin	Assignment
1	TX +	5	Not connected
2	TX -	6	RX -
3	RX +	7	Not connected
4	Not connected	8	Not connected

A.3 RJ 45 Connector ISDN

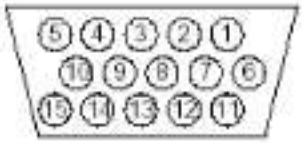


Pin	Assignment	Pin	Assignment
1	Not connected	5	RX -
2	Not connected	6	TX -
3	TX +	7	Not connected
4	RX +	8	Not connected

A.4 Serial SUB-D 9 Connector 1

Pin	Assignment	Pin	Assignment
1	DCD	6	DSR
2	RX	7	RTS
3	TX	8	CTS
4	DTR	9	RI
5	GND		

A.5 KVM 15 pin connector



Pin	Assignment	Pin	Assignment
1	VGA Red	9	MS Data
2	VGA Green	10	KBD VCC
3	VGA Blue	11	MS Clock
4	KBD Data	12	SDA, DCC, ...
5	KBD Clock	13	HSYNC
6	GND	14	VSYNC
7	GND	15	DATA_CLOCK
8	GND		

B. Video Modes

Table B.1 lists the video modes BI080135/BI160135 supports. Please don't use other custom video settings besides of these. If done so, BI080135/BI160135 may not be able to detect them.

Resolution (x, y)	Refresh Rates (Hz)
640 x 350	70, 85
640 x 400	56, 70, 85
640 x 480	60, 67, 72, 75, 85, 90, 100, 120
720 x 400	70, 85
800 x 600	56, 60, 70, 72, 75, 85, 90, 100
832 x 624	75
1024 x 768	60, 70, 72, 75, 85, 90, 100
1152 x 864	75
1152 x 870	75
1152 x 900	66
1280 x 960	60
1280 x 1024	60, 75

Table C.1 Video mode

BMND20000